MDT software
the change management company

AutoSave

Achieving Part 11 Compliance

A White Paper

steflex

Synopsis

This whitepaper provides information related to FDA regulation 21 CFR Part 11 (Part 11) for organizations considering MDT software solutions. The intent is to establish a mutual understanding of the rules set forth in Part 11 and explain how MDT can help their customers comply with the rules. This whitepaper was written by Stelex, Inc. based upon AutoSave Version 5.03 released March, 2006.

Part 11 Review

Part 11 establishes the criteria under which electronic records and electronic signatures are considered as equivalent to paper records and handwritten signatures executed on paper. The rule applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations.

In order for organizations to comply with Part 11, requirements of authenticity, integrity, and confidentiality of the records and signatures must be met. Any computer system utilizing electronic records and signatures must be validated according to generally accepted industry standards associated with a Software Development Life Cycle (SDLC) to ensure its accuracy, reliability, consistent intended performance, and ability to discern invalid or altered records.

Several checks must be built into a Part 11 compliant system including:

- System checks that enforce the sequencing of events, where required
- Authority checks that determine who has access to the system and at what level
- Device checks that determine the validity of sources of data being entered into a system

The system must also be able to independently generate audit trails that describe who accessed the system and what operations were performed during any given period. The audit trails must be secured, computer-generated, time-stamped, not obscure previously recorded data, identify the person making the change, include original and changed data, and be available for review and copy by FDA. Audit trail documentation thus generated is required to be retained for a period at least as long as that required for the subject electronic records, either pursuant to a predicate rule or to the organization’s own records retention policy.

Part 11 also sets forth requirements for electronic signatures. Each electronic signature used within an organization must be unique to an individual and not reused or assigned to another. The identity of the individual must be verified by the organization (e.g., via birth certificate, driver’s license, passport) before assigning the individual an electronic signature. The organization must also certify in writing to FDA that they intend to use their electronic signature as the legally binding equivalent of their handwritten signatures. This certification must be submitted to FDA in paper form.

Risk Assessment

As a result of industry feedback, FDA modified its position on Part 11 in 2003. With streamlined enforcement and restricted interpretation by FDA, organizations must still comply with predicate rules regarding validation, audit trails, retention, copying, and legacy systems. The primary change in FDA guidance involves risk assessments performed in each of these areas. The new emphasis upon a risk-based approach places the onus on industry to identify the risks and to determine appropriate actions.

Organizations should have written procedures for identifying, specifying, and documenting the risk assessment techniques and risk mitigation methodologies to be used during the design and development of computer controlled systems. The intent is to detect potential design flaws (i.e., possibilities of failure that could cause harm to personnel, the subject system, or the environment) and to enable manufacturers to correct these failures before a product is commercially released.

It is beneficial to first determine which requirements have potential risks associated with them. Then the potential risk and possible cause should be identified. As an example, risk severity, likelihood, and its ability to be detected can be quantified. Risk severity could be rated from negligible to high with associated sequential numbers and criteria for each. Risk likelihood could be rated from improbable to frequent and so forth. The results from these types of ratings can be used to calculate a risk index that would then be the basis of a risk mitigation plan.

MDT's Commitment to Regulated Industry

Programmable Logic Controllers (PLCs) are the backbone of automated manufacturing in the pharmaceutical, biotechnology, and medical device industry. With AutoSave, MDT has a substantial history as a world leader in automation change management supporting the most comprehensive range of PLC devices and editors. These devices are programmable and rely on digital programs that define their functionality and operation. The programs are stored electronically in the device and on backup electronic media. For this reason they are considered electronic records and fall under the requirements imposed by 21 CFR Part 11. Methods for conventional office records tracking and change control would not be sufficient for records associated with programmable devices.

It is not uncommon to find that PLCs are supplied by a variety of manufacturers where each brand comes with a unique set of program development and device management tools. Add to this the many legacy systems installed in an operating plant and one begins to understand the enormity of the change control and program archiving problem.

The program files represent the result of hundreds of worker hours. If a device fails or a program is lost, the inability to restore the last known working version can result in substantial economic loss in the form of production down-time.

The AutoSave server stores all programs for access during crisis situations. The server is solely responsible for system security and privilege control, archiving versions and ancestors, managing program files, and creating audit trails for historical tracking.

For each PLC connected to the network, the AutoSave Server records:

1. The type of device
2. Where the device is located on the network
3. The type of software that is used to program the device
4. Who is authorized to access that device and the changes they are authorized to make.
5. Previous copies or ancestors of the production copies. Multiple previous versions may be archived.
6. Master copies or named versions of the programs

When a user wishes to work with a specific PLC, AutoSave works with the client in the following sequence:

1. Technician logs in and requests the right to work on the network by entering a user name and password.
2. The AutoSave server reviews the user's privileges and the AutoSave client displays the devices and programs the user is authorized to access. User requests a device and control program and AutoSave server grants access and downloads the required files. The files are marked at the server as being locked and checked-out. Requests by other clients to access those files will be denied.
3. AutoSave client then starts the programming editor application required to work with the selected device and then connects to the offline or online PLC through the field network.
4. The user then works offline or online with the selected PLC, making the required modifications.
5. When complete, the changes can be optionally uploaded from the PLC to the client (if performed online).
6. The user then annotates the change record, including a mandatory record of the reason for the modification.
7. Together with the modification record, the new copy of the program file is uploaded from the client to the server. The server automatically moves the previous version to the ancestor files and saves the new version as the current version. The server then writes the audit trail for the user's session.
8. The AutoSave server then sends an email to the individuals who need to be advised that a change was made. Typically these will be sent to responsible individuals in Engineering, Production, QC, and Validation.

The reader will note that even remote laptops are controlled in the AutoSave change control environment. However, it is possible for a technically capable individual with a private copy of the manufacturer's support software to get in and make an uncontrolled change. To protect against this, AutoSave Server periodically connects to each device through the enterprise and proprietary networks and checks the actual contents of the device against the copies stored on the server. If these are ever different, notifications go out immediately. Under the change control environment established by AutoSave, the following benefits are realized by the Part 11 regulated organization:

1. All electronic files and program copies associated with Programmable Devices reside in one location, the AutoSave Server. Backup is controlled and automatic so any uncertainty of manual backups is eliminated.
2. Access by any individual to the program files and the devices themselves is tightly controlled from one location, the AutoSave Server. Electronic signature protection in accordance with 21CFR Part11 can be provided. The user need not worry about establishing authorization through the different types of device support workstations needed to access multiple brands of PLCs. Prior authorization at the AutoSave server level is required for anyone to access this information.
3. The steps performed during a user's session on an AutoSave client workstation must be accomplished in a consistent and repeatable fashion. Activities resulting in saved files at the client must be annotated with the extent of the changes and the reasons for them. Also, changes must be performed within the time window of the AutoSave client.
4. All file storage and version archiving is performed automatically in a tightly controlled environment. The proper audit trails are created transparently and human error cannot factor into the process.
5. Audits can be conducted simply at any time. AutoSave has a comprehensive Web Reports application to allow change histories to be extracted from the system. For many of the more popular PLC's, AutoSave will also annotate the PLC program documentation with the specific changes made, whether or not the technician making the change annotated the program. For users who want additional data, the Web Reports package provides additional comprehensive reports.
6. When a change is made to a program, individuals who need to know are notified by email. The individual's name, device name, time and date of the change, and the reason for the change are included in the email.
7. Programmable device programs are automatically checked for integrity on a scheduled basis. Any deviation from the expected version will be flagged immediately and the proper individuals notified.
8. If a disaster occurs, management is assured the program can be restored quickly and the version reloaded is identical to the previous one. Likewise, if a new version is faulty, restoration of the previous version is made quickly. Downtime is minimized and the potential for disaster is eliminated.
9. The cost expended to develop a program, test, debug, and validate it can not be lost and will not have to be duplicated. In essence the value of this intangible but expensive asset is assured.

The following table is based on the requirements of Part 11 and the AutoSave application assessed for its applicability and level of compliance:

Section #	Requirement	Compliance/Documentation/Comments
		MDT AutoSave Software
B/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. **NOTE:** *The FDA intends to exercise enforcement discretion regarding this requirement for Part 11, though persons must still comply with applicable predicate rule requirements for validation. The FDA recommends that validation be based on a justified and documented risk assessment.*	N/A Notes: Each client will have a unique approach to validation and are responsible for validating their individual AutoSave implementations. MDT can provide information to assist in the effort. Internally, AutoSave has undergone rigorous testing governed by internal MDT testing protocols. As of AutoSave Version 5.03 there have been no Part 11 deviations per QA procedures.
(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. **NOTE:** *The FDA intends to exercise enforcement discretion regarding this requirement for Part 11; persons should provide an investigator with reasonable and useful access to records during an inspection ensuring the copying process produces copies that preserve the content and meaning of the record.*	Reports generated using the AutoSave Software can be viewed on any connected Client PC and also when printed to a connected printer.

Section #	Requirement	Compliance/Documentation/Comments
		MDT AutoSave Software
(c)	**Protection of records** to enable their accurate and ready retrieval throughout the records retention period. **NOTE:** *The FDA intends to exercise enforcement discretion regarding this requirement for Part 11. The FDA suggests the decision on how to maintain records be based on predicate rule requirements and on a justified and documented risk assessment.*	Records are maintained in a secure relational database retrievable using a variety of database reporting tools. Record retention periods can be defined and configured based on standard business procedures.
(d)	**Limiting system access** to authorized individuals.	Access is limited to the list of users present in the User Administration menu of the interface. Users have privileges associated with their login information making it possible to limit certain functions only to specific users.
(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. **NOTE:** *The FDA intends to exercise enforcement discretion regarding this requirement for Part 11, though persons must still comply with applicable predicate rule requirements related to documentation of, for example, date, time, or sequencing of events. FDA states even if no predicate rule exists for this requirement, it may still be important to have audit trails or other security measure to ensure the trustworthiness and reliability of the records.*	The system maintains an "Activity Log" that tracks the user actions and changes in program versions. Audit trails are stored in relational database tables. The persistent tables, LG_Sys and LG_Approval, log messages written by the system and those in support of Part 11 features respectively. All activities (performed by the user or by the system) can be accessed/ viewed through a set of reports present in the Reporting Module of the application. Audit Trails cannot be bypassed or disabled by users.
(f)	**Use of operational system checks** to enforce permitted sequencing of steps and events, as appropriate.	Steps are enforced with respect to checking in and checking out programs and also with creating ancestor versions of programs stored within the AutoSave database.

Section #	**Requirement**	**Compliance/Documentation/Comments**
		MDT AutoSave Software
(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.	Access is limited to the list of users present in the User Administration menu of the interface. Users have privileges associated with their login information making it possible to limit certain functions only to specific users.
(h)	**Use of device** (e.g., terminal) **checks** to determine, as appropriate, the validity of the source of data input or operational instruction.	The list of devices connected to the AutoSave server needs to be configured upon install and data is transferred between the server/ client PC and the device only for the specified devices. Each device is assigned a unique IP address thus ensuring the validity of the data transfer between the device and the software.
(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems **has the education, training, and experience to perform** their assigned tasks.	Training on use and maintenance is available from MDT. Training in application and operator training is also available from MDT.
(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** Customers are responsible for developing policies and procedures that hold individuals accountable and responsible for actions initiated under their electronic signature.
(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**.	The client is responsible for this procedural control as it pertains to documentation that can be modified by the client. The client cannot modify MDT copyrighted material.
(2)	**Revision and change control procedures** to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Client developed and/or modified electronic documentation must follow approved change control procedures that include audit trail information per Part 11. This does not pertain to MDT copyrighted material.

Section #	Requirement	Compliance/Documentation/Comments
		MDT AutoSave Software
B/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.	**N/A**
B/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**	The Activity Log contains the User ID associated with each event/action.
(2)	The **date and time** when the signature was executed; and	The Activity Log contains a date/time stamp associated with each event/action.
(3)	The **meaning** (such as review, approval, responsibility, or authorship) associated with the signature.	The Activity Log contains the details of the events/ actions performed (approval, responsibility, authorship).
(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).	The Activity Log contains the User ID/time stamp and the details of the action performed associated with each event/action.

Section #	Requirement	Compliance/Documentation/Comments
		MDT AutoSave Software
B/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.	Each User ID has a unique password associated with it ensuring that the signatures cannot be excised, copied or transferred to falsify an electronic record.
C/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.	System access is based on unique User ID/ password combinations. Customers should ensure procedures are in place to prevent reuse and/or reassignment of User ID's.
(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** Customers are responsible for the verification of the identity of the individual before an electronic signature is assigned and/or sanctioned.
(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.	**N/A** Customers are responsible for certification to FDA that the electronic signatures used at their establishment are intended to be the legally binding equivalent of 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.	**N/A** Customers are responsible for the submission of the certification to FDA with a traditional handwritten signature.
(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 Customers are responsible for providing certification or testimony that an individual's electronic signature used at their establishment is the legally binding equivalent of their handwritten signature.

Section #	Requirement	Compliance/Documentation/Comments
		MDT AutoSave Software
C/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.	Each User ID has a unique password associated with it ensuring that the electronic signature has two distinct identification components.
(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.	The User ID and password are required to login and also to perform subsequent actions ensuring that at least one electronic signature component is required by an individual executing an electronic signature at any given time of use.
(ii)	When an individual executes **one or more signings not performed during a single, continuous period** of con-trolled system access, each signing shall be executed using all of the electronic signature components.	The User ID and password are required to login and also to perform subsequent actions ensuring that at least one electronic signature component is required by an individual executing an electronic signature at any given time of use.
(2)	Be **used only by their genuine owners**.	System access is granted based on a unique combination of User ID and password issued to only authorized users.
(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.	System access is granted based on the unique combination of the User ID and password ensuring that the use of an electronic signature by anyone other that its genuine owner will require the collaboration of two or more individuals.
(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** No biometrics used.

Section #	Requirement	Compliance/Documentation/Comments
		MDT AutoSave Software
C/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.	The User ID and password combination allows the user to access the application based on the privileges associated with the User ID ensuring that no two individuals have the same set of credentials to gain access to the system.
(b)	Ensuring that **identification code and password issuances** are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Customers are advised to implement procedures to periodically check, recall and revise the passwords issuances and to use the built in features of Windows Active Directory for password aging and history control.
(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.	**N/A** Token cards or other devices that generate identification code or password information are not currently used.
(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.	Customers are advised to use the in-built features of Windows Active Directory to implement transaction safeguards to ensure that there is no unauthorized use of passwords and User IDs. Windows Active Directory will also allow system administrators to be notified, in an immediate manner, of any attempts of unauthorized use. It is further recommended that procedures be put in place for regular inspection of the operating system event log to detect such attempts.

Section #	Requirement	Compliance/Documentation/Comments
		MDT AutoSave Software
(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** Token cards or other devices that generate identification code or password information are not currently used.

About MDT Software

MDT Software is the world leader in change management solutions for automated manufacturing assets. Founded in 1987, MDT Software has consistently delivered innovative solutions that are now considered benchmarks of excellence in industrial automation. MDT focuses solely on change management software solutions for the industrial marketplace, and does not develop PLC, SCADA or DCS products. This independence enables MDT to address its client's change management needs objectively. Today, over 4,700 end users in a broad variety of industries worldwide have made AutoSave software their response to the challenge of effectively managing an increasing quantity and array of software on the plant floor. MDT Software is headquarted in Alpharetta, Georgia, USA and works with distributors and integrators worldwide.

www.mdtsoft.com
678.297.1000

About Stelex

Stelex provides enterprise-wide compliance solutions to regulated industries in the pharmaceutical, medical device, diagnostic and biotechnology sectors. The firm delivers a comprehensive suite of validation, technology, regulatory and business solutions. In addition to quality auditing services, Stelex offers Sarbanes-Oxley Compliance consulting, System Integration and Implementation, Security & PKI services, Computer System Validation, Process Validation, Equipment Qualification, Infrastructure Qualification, Program Management, Best Practice Consulting, and a broad range of technical training and professional education through fully accredited Stelex University.

Stelex's corporate office is located in Bensalem, PA, with regional offices in Puerto Rico, Massachusetts, New Jersey and Illinois. Since 1986, Stelex has built its reputation on the long-term relationships established with both its clients and partners. Stelex is positioned to be your total compliance solutions provider.

www.stelex.com
215.638.9700

About the Author

Stephen Dallas is a Project Manager at Stelex in the Pennsylvania office where he has managed long-term Quality Management and Compliance Assessment projects for major pharmaceutical companies. He has also helped Stelex establish strategic partnerships with companies who supply various industries with enterprise solutions.