Sympatec GmbH
System-Partikel-Technik

WINDOX 4

Electronic Records/ Electronic Signatures Compliance Assessment Worksheet for 21 CFR Part 11

Note

Complete or partial duplication of the present documentation and software without written permission is prohibited. Rights to the documentation and software are reserved by Sympatec GmbH.

Since complete freedom from error in technical documentation is rarely achievable in spite of the greatest care, no warranty is hereby implied for the absolute accuracy of this document. Sympatec would be grateful to be advised of any corrections required.

Goslar, 25. April 2002.

Content

1 Introduction

The Sympatec software WINDOX 4 has been designed to provide all technological controls required to achieve compliance with *21 CFR part 11*.

Purpose

This assessment worksheet has been compiled with the kind help of *Mr. H. Garston Smith*, an international software quality assurance auditor and consultant within the global pharmaceutical industry, to whom Sympatec express their grateful thanks for permission to use it.

All information not relevant to Sympatec's instruments, hardware and software has been stripped from the original worksheet. Therefore, the worksheet does not claim to cover all aspects of an assessment. Emphasis is laid on how software technology supplied with Sympatec's system can support the company's efforts to become compliant, i.e.

- Specify the criteria under which computer systems are to be evaluated against 21 CFR Part 11.
- Help users of the Sympatec particle size analysis systems to become compliant with the rule.

Scope

The assessment worksheet must be completed for:

- Records and signatures required by the FDA that are created, modified, maintained, archived, retrieved, or transmitted in electronic form.
- Records and signatures which may be submitted to the FDA in electronic form, whether required by FDA regulation or not.
- Signatures applied electronically to FDA required records or records that may be submitted to FDA, even if the signatures are not required by FDA regulation.

Use

Please carefully read chapter 2 for further information.

We wish you every success!

2 Instructions for use of the Assessment Worksheet

2.1 Part I (System Information):

1. Indicate the System Name and Version Number.
2. Complete Section **E (Computerized (Automated) Equipment)** for Computerized (Automated) Equipment.

2.2 Part II (System Assessment): This includes Sections G, I, and J.

1. Complete **Section G (Initial Questions)** (Questions Q1 through Q3). Continue with the subsequent steps (2 – 7) based on the results obtained in this section. The information in these sections is **MANDATORY**.

2. Complete **Section I (Assessment)**.

   The Document *GAMP SIG Complying with 21 CFR part 11 (Final Draft)* distinguishes between company operating procedures that will be required and technological controls that are required of Electronic Record and Electronic Signature (ERES) systems. To achieve compliance, a combination of both types of controls is necessary.

   Sympatec has preset a **"S:Yes"** or **"S:No"** in the **Assessment Result** column if the requirement addresses technological controls. All preset answers apply to the Software WINDOX 4, Version 1, Release 2, or later versions/releases, if set up in "CFR part 11 mode".

   A **"P:___"** in that column indicates that it is up to the pharmaceutical company to provide a required procedural control. Whenever possible, Sympatec has noted a proposal of a suitable procedural control in column **Remarks**.

   After implementing the required procedural control, assess the ability of the system to fulfil the specified 21 CFR Part 11 requirement. Record **"Yes"** or **"No"** behind the **"P"** in the **Assessment Result** column.

   Use the **Remarks** section to provide references and explanations for the Assessment Result regardless of its content. **Remarks must be provided to substantiate the response.**

Example of the use of explanatory remarks

Assessment Result	Remarks
The data center is managed by an outside vendor and located on his premises. However, the company owns the servers and entirely controls the access to them.	The system Initially appeared to be OPEN under the 21CFR 11 definition. However, the access controls in place were secure and documented, so the system could actually be considered to be CLOSED.

3. Complete Section J (Classification) based on the completion of Section I (Assessment).

3 Worksheet PART I: System Information

System Name:	**Sympatec HELOS with Software:**	**WINDOX 4**
	Version Number :	**3 1.3**

3.1 Section A (Pre-Assessment Meeting Information)

P:___	**no contribution possible within the scope of this document**

3.2 Section B (General Information for All Systems)

P:___	**no contribution possible within the scope of this document**

3.3 Section C (Record and Report Information for All Systems)

P:___	**no contribution possible within the scope of this document**

3.4 Section D (Information System)

N/A	**not applicable to Sympatec systems**

3.5 Section E (Computerized (Automated) Equipment)

Product / Equipment Name	**HELOS**
Product / Equipment Vendor	**Sympatec GmbH**
Model Number	**N/A**
Controller Make and Model	**N/A**
Software or Ladder Logic Version or Date	**WINDOX 4, 3 1.3**
Circle one: Ladder Logic or Software is…	**Unmodified from Vendor**
Computer Hardware	**Compatible PC**
Operating System Name and Version	**MS Windows NT4™ or Windows 2000™**

™ WINDOWS NT and WINDOWS 2000 are Trademarks of the Microsoft Corporation.

3.6 Section F (External Devices)

N/A	**not applicable to Sympatec systems**

4 Worksheet PART II: System Assessment

4.1 Section G (Initial Questions)

4.1.1 PART 11 Applicability Questions

Reference	Question	Assessment Result	Remarks
Q1	• Does this computerized system create, modify, maintain, archive, retrieve, or transmit any electronic records(s) that are required to demonstrate compliance with FDA regulations or that generate data that is required by or submitted to the FDA?	S:Yes	If the answer to the question is “No”, then this system is NOT subject to the regulation under Part 11, and the rest of this questionnaire should not be completed. If the answer to the question is “S:Yes”, then indicate the Predicate Rule and section which applies: 210 sec 185
Q2	• Do FDA regulations permit the use of electronic records for this required documentation? If the answer is “No”, indicate the specific CFR reference requiring these records to be maintained in paper format only. ____ CFR Part(s) _____	P:___	If the answer to the question is “No”, then this system is NOT subject to the regulation under Part 11, and the rest of this questionnaire should not be completed.
Q3	• Is the computerized system (all components) a closed system whereby data and system access is solely controlled by the user companies personnel (including their agents) who are responsible for the content of the electronic records on the system?	S:Yes	If the answer to the question is “Yes”, then skip 11.30. If the answer to the question is “No”, then it is considered to be an open system, and 11.30 must be addressed.

4.2 Section H (Assessment Meeting Information)

P:___	**no contribution possible within the scope of this document**

4.3 Section I (Assessment)

4.3.1 Electronic Record (Closed System)

Reference	Question	Assessment Result	Remarks
11.10(a) Preamble clauses 64-68	• Has the system been validated in order to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?	S:Yes	Documentary evidence e.g. IQ/ PQ/OQ is provided upon request.
	• When was it last validated or revalidated? (reference QPGs here)	P:__.__.__	Please enter the date of validation of your software version. e.g. 20.06.2001 for WINDOX 4.1.2.
	- Was an established software development life cycle used?	S:Yes	Documentary evidence e.g. IQ/ PQ/OQ is provided upon request.
	- Does a requirements document exist?	S:Yes	
	- Does a design document exist?	S:Yes	
	- Have code reviews been conducted?	S:Yes	
	- If developed in-house, has developer testing been conducted?	S:Yes	
	- If vendor supplied, has an audit of the vendor been conducted?	S:Yes	
	- Has System Testing been conducted?	S:Yes	
	- Has User Acceptance Testing been conducted?	S:Yes	
	- Has Installation Qualification Testing been conducted?	S:Yes	
	- Has Operational Qualification Testing been conducted?	S:Yes	
	- Has Performance Qualification Testing been conducted?	S:Yes	

Reference	Question	Assessment Result	Remarks
11.10(a) (continued) Preamble clauses 64-68	- Is there a formal training plan?	S:Yes	Documentary evidence e.g. IQ/ PQ/OQ is provided upon request.
	- Has Performance Qualification Testing been conducted?	S:Yes	
	- Is there a support plan?	S:Yes	
	- If this is a legacy system, has a Part 11 assessment been conducted?	S:Yes	
	- Does a Change Control procedure exist?	S:Yes	
	- Does evidence exist that it was followed ?	S:Yes	
	- Does it cover changes to all system components?	S:Yes	
	• Are these documents kept in electronic format?	S:Yes	
	• If so, is the document management system Part 11 compliant?	S:Yes	
	• Did validation include testing that the system discerns invalid records (i.e. invalid field entries, fields left blank that should contain data, values outside of limits, ASCII characters in numeric-only fields, etc)?	P:___	
	• Did validation include testing that the audit trail records altered (create, modify, delete) records properly?	P:___	
	• Review the validation package (add comments).	P:___	
11.10(b) Preamble clauses 69-70	• Is the system capable of generating accurate and complete copies of all required records in both human readable and electronic form suitable for inspection, review and copying by the FDA?	S:Yes	Human readable form: Reports on a printer or into text files, configurable by templates, so the degree of completeness depends on the template used for the report. Electronic form: Database export function.

Reference	Question	Assessment Result	Remarks
11.10(b) (continued) Preamble clauses 69-70	• Can a copy of a single record (in electronic format) be supplied to an inspector? In paper format?	S:Yes	Electronic format: Database export function. Paper format: Report.
	• Can a copy of the entire database (in electronic format) be supplied to an inspector?	S:Yes	The database is a directory of files. It can be copied onto any medium with the operating system's file explorer.
	• Are procedures in place to describe HOW to accomplish these inspection tasks?	S:Yes	We recommend to use the Service Request Wizard. It creates a compressed copy of all necessary files.
	• Are procedures in place to define what in format the electronic records will be provided?	S:Yes	On-line-Help contains a description of all Report template statements, their value and format.
11.10(c) Preamble clause 71	• Are the records protected to ensure their accurate and ready retrieval throughout the record retention period?	S:Yes	No measured data or data describing the circumstances of the measurement can be deleted from the database. If the database format is changed due to an update, a conversion utility is provided to ensure compatibility of old data.
	• Are records protected on the system to prevent unauthorized modification or deletion?	S:Yes	
	• Are data files written to a protected directory or database table such that only personnel with high-level access privileges can access the data files?	P:___	Due to restrictions of the Microsoft Windows NT or 2000 operating systems, it is not possible to distinguish between data access through the software supplied by Sympatec, and access through other programs. This means, all users of the Sympatec software must have write access to the data directory to be able to save measured data. The deletion of files or directories however, should be granted to privileged users only. This is a system administrator's task.
	• Do system users have access to the data files or database records, such that they could accidentally or intentionally modify or delete data files?	P:___	
	• Has any capacity planning been performed?	P:___	On modern PC's storage capacity is not a problem. After some time of use, however, the size of the database directory should be checked and compared to the amount of free space on disk.
	• Is there a written records retention policy?	P:___	
	• Does it include electronic records?	P:___	
	• Does it include audit trails?	P:___	

Reference	Question	Assessment Result	Remarks
11.10(c) (continued) Preamble clause 71	• Describe the backup and restore process. Is there an SOP?	P:___	
	• Describe the data archiving process. Is there an SOP? If no, is all data kept on-line?	P:___	The Sympatec WINDOX software provides powerful functions to export and/or archive data records.
	• Does the SOP and actual practice ensure the archived data is controlled and maintained for the required retention period?	P:___	
	• Are any backups and/or archives duplicated (e.g., to create off-site backups/archives for disaster recovery)? How is this media protected?	P:___	
	• Is the meta-data stored with the archived data?	S:Yes	All data necessary to recalculate the measured results is stored.
	• Is virus software loaded and regularly updated to prevent viruses corrupting data?	P:___	
11.10(d)	This requirement refers to both logical and physical access. • Is system access limited to authorized individuals?	P:___	
	• Is a username/password (or other logical security) required to access the system?	S:Yes	Provided by the operating system Windows NT or 2000
	• Is there a security SOP that covers physical and logical security, access authorization, modification, disabling/deleting periodic checking of access, approval by System Owner?	P:___	
	• What controls limit physical access to the system?	P:___	
	• Is there firewall protection to prevent *un*authorized access from the Internet?	P:___:	

Reference	Question	Assessment Result	Remarks
11.10(e) Preamble references 72, 73, 74, 75, 76, 77, 78, 93	• Is there a secure, computer-generated, time-stamped audit trail that independently records the date and time of operator entries and actions that create, modify, or delete electronic records?	S:Yes	Every data record is marked with date, time, and user ID in the moment of its creation. Records can be divided into four types: • meta data of the system (mainly properties of the measured powder): Such data can be changed at any time, but access to the data can be blocked for everyone by the system administrator. An audit trail of subsequent modifications is generated in the - write-protected - comment field of the data. • description of the measurement setup and free user parameters: Such data can be altered as long as no measurement has been performed using these data. When used in a measurement, such data can no more be altered or deleted. Alternatively, write access to such data can be totally blocked by the system administrator. This is not recommended. • measured data. Such data can never be modified or deleted. • free commentary information. It is possible to add commentary information at any time but not to modify or delete existing comment. Every amendment is marked with date/time and user ID. This is the audit trail of modifications to the commentary information.
	• Upon making a change to an electronic record, is previously recorded information still available?	S:Yes	
	• Are electronic audit trails kept for a period at least as long as their subject electronic records and available for agency review and copying?	S:Yes	

Reference	Question	Assessment Result	Remarks
11.10(e) (continued) Preamble references 72, 73, 74, 75, 76, 77, 78, 93	For each type of record in the system, please address the following questions:		Types of records are: a) System data (e.g. detector number) b) Meta-data (product properties) c) Measuring conditions d) Measured data e) User parameters f) Comment to the measurement After a measurement has been performed, all related records except types b) and f) are automatically write-protected.
	• Does the system generate automatic, electronic audit trail information (who, what, when)?	S: type b) Yes	Type b) Every modification of the meta data is logged by User ID, date and time, and what was modified.
		S: type f) Yes	Type f) Who and when is logged by User ID, date and time. “What” can only be creation or amendment, which is self explanatory and therefore not extra logged.
	• Does the audit trail include the reason for change (if required by the predicate rule)?	S: type b) No	The user can but need not add a commentary information about the reason for change.
		S: type f) Yes	Creation or amendment is self-explanatory in the record itself.
	• Is the audit trail function always ON, or is it turned OFF and ON manually? If manual, who and what triggers audit trail recording? Does it get turned on early enough in the process? Is it reliable (i.e., can they forget to turn it on)?	S:Yes	It is on when the program is in “CFR rule 11 mode”. This mode should permanently be ON. Only the administrator can switch it OFF, but this is never necessary. So the risk to leave it switched OFF inadvertently can be neglected.
	• Does the audit trail capture every user action that creates, modifies, or deletes records, without exceptions?	S:Yes	Due to the fact that modification and deletion is not possible when the software set-up complies with the above-mentioned recommendations, only creation of records and amendment of comments must be captured. This is done reliably.
11.10(e) (continued) Preamble	• When information is changed, does the audit trail record/save the previous value?	S:Yes	

Reference	Question	Assessment Result	Remarks
references 72, 73, 74, 75, 76, 77, 78, 93	• Are audit trail entries made at the time the action/operation was conducted electronically?	S:Yes	
	• Is the audit trail ever monitored or reviewed to detect possible misuse or unauthorized activity?	P:_____	The logging of modifications is fully transparent to the user.
	• Is it possible to reconstruct events (delete, modify, etc) to any point in time by only using the audit trail information and the original record?	S:Yes	Only the original record is necessary, which carries its individual audit trail information. The record is always write-protected, so a deletion need not be reconstructed.
	• Are electronic audit trails (all or any part) readily available for FDA review and copying? In paper format?	S:Yes	See above. The record itself contains its audit trail information in the commentary info field.
	• Does the audit trail contain date and time stamps? Can time local to the activity be derived?	S:Yes P:___	The system uses the local time of the PC's operating system. A procedural control must define which time this is.
	• Are meaningful units of time chosen in terms of documenting human actions? (For example, seconds might be used in a data collection system while minutes might be appropriate for a document management system.)	S:Yes	
	• Is the audit trail completely transparent to, and outside the control and access of, the user?	S:Yes	(see above) The audit trail data is contained in the commentary info field of the respective data record which cannot be modified or deleted but only extended by amendments. So it is transparent and write-protected.
	• How is audit trail data protected from accidental or intentional modification or deletion?	S:Yes	
11.10(e) (continued) Preamble references 72, 73, 74, 75, 76, 77, 78, 93	• System Administrators and DBA's typically make changes. Do those changes have audit trails? If not, do procedural controls exist over use of such administrator tools?	S:Yes P:___	All actions of granting or blocking user rights of the Sympatec software are logged in an administration log file. A procedural control is recommended describing how to handle the administration log file, because it cannot protected from access by the administrator.

Reference	Question	Assessment Result	Remarks
	• Does the records retention program cover audit trails?	S:Yes	
	• Are electronic audit trails kept for at least as long as their respective electronic records?	S:Yes	
	• What ensures that the system time and date are correct? How frequently are the time and date synchronized with a reliable source?	P:___	It is recommended that the system administrator disables the feature to change the system date and time for all users except the administrator. This can be done by the local security policy or the policy of the network domain.
	• Can users readily change the system time/date?	P:___	
	• Are time/date stamps applied by the local workstation or by a server (or equivalent)?	P:___	
11.10(f) Preamble references 59, 79, 80, 81	• Are operational system checks used to enforce permitted sequencing of steps and events?	S:Yes	The sequence of operation is not totally rigid. But some operational steps must precede/follow other steps. Only allowed operational steps are enabled, all operation that does not make sense in a certain context is blocked, or error messages are displayed if an attempt to violate the proper sequence is made.
	• Are there sequences of operations, or sequential events, or sequential data entry, that is important to this system? - If so, what are they? - If so, how does the system ensure that steps are followed in the correct sequence?	S:Yes	
11.10(g) Preamble references 82, 83, 84	This requirement refers to functional access once a user logs into the system • Are authority checks in place 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?	S:Yes P:___	The operating system Windows NT or 2000 features a full access control including audit and action in case of fraud. The WINDOX4 software relies on this access control. The pharmaceutical company's system administrator grants or restricts access rights to the application software and the files or directories.

Reference	Question	Assessment Result	Remarks
	• Are there different levels of access based on user responsibilities? - If so, what are they?	S:Yes	System administrator (all rights including administration of user access rights) Power User (can use the WINDOX4 software but cannot modify user access rights) Ordinary user (can not use the WINDOX4 software)
	• Is there an SOP describing how these are assigned, documented and controlled?	P:___	All users of the WINDOX4 software should be qualified as Power Users and be granted write access to the database directory. To prevent inadvertent loss of data, the right do delete files or directories of the database should be blocked for all users except the administrator.
	• What process is followed to grant a new user access to the system, or to change privileges for an existing user? Is it documented?	P:___	
	• Are levels of access periodically reviewed?	P:___	
	• Are authority checks used to ensure that only authorized individuals can use the system?	P:___	The system administrator can grant or restrict the right to use the WINDOX 4 software, and can set the program's operating mode (CFR rule 11 compliant or not). All users who are allowed to use the software have equal rights within the software, even the administrator. These rights have been described above (section 11.10 c)
	• Are authority checks used to ensure that only authorized individuals can electronically sign a record?	P:___	
	• Are authority checks used to ensure that only authorized individuals can access the operation or computer system input or output devices?	P:___	
11.10(g) (continued) Preamble references 82, 83, 84	• Are authority checks used to ensure that only authorized individuals can alter a record ?	P:___	
	• Are authority checks used to ensure that only authorized individuals can perform the operation at hand?	P:___	

Reference	Question	Assessment Result	Remarks
11.10(h) Preamble references 59, 85	• Are device checks used to determine, as appropriate, the validity of the source of data or operational instruction? • Is it necessary to ensure that the data source is identified? If so, what are they? If so, how are they identified? *Example – console commands for a server are limited to the console station* *Another example – modem access may be verified to ensure the identify of the caller*	N/A	The system is operated locally by the user who has most recently logged in. No further check is necessary.
11.10(i) Preamble references 86, 87	• Is there documentation to show that persons who develop, maintain, or use electronic records/signature systems have the education, training, and experience to perform their assigned tasks?	S:Yes	
	• For internal persons, is there evidence that they are qualified for their job? (This requirement may be met with CVs, job descriptions, training records, and a training procedure that is followed)	S:Yes	Only staff with university degree are employed for software development.
	• For external persons, is there evidence that they are qualified to perform the work for which they were hired? (This requirement may be met by having their resume on file)	S:Yes	
	• Is there an SOP covering user training?	S:Yes	

Reference	Question	Assessment Result	Remarks
11.10(i)	• Is there evidence of user training?-	S:Yes	
	• Are there SOPs, company requirements, job descriptions, etc., that describe minimum educational requirements and/or work experience for system developers? Support staff?	S:Yes	
	• What evidence exists of suitable qualifications and/or proficiency for developers and support personnel?	S:Yes	University degrees in engineering, mathematics or computer science.
	• Is there any system training for developers and/or support staff?	S:Yes	
11.10(k) Preamble references 78, 92, 93	• Are there adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance?	P:___	
	• Are there formal revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation?	S:Yes	
	• Is there a list of system documentation related to the operation of the system that exists (e.g., SOPs, procedures covering the creation of user accounts and backups, etc.)?	P:___	
	• Is there a list of system documentation related to the development of the system that exists (e.g., requirements, design specifications, training materials, etc.)?	S:Yes	

Reference	Question	Assessment Result	Remarks
11.10(k) (continued) Preamble references 78, 92, 93	• Is the system documentation maintained by the pharmaceutical company's revision control so changes can be determined and the history of the documents is obvious?	P:___	
	• Are old copies of vendor documentation maintained to provide a complete history of the system?	P:___	
	Is access to Design documentation restricted?	S:Yes	Some documentation is not published but can be reviewed at Sympatec's factory.
	Are these documents kept in electronic format?	S:Yes	
	- If so, is the document management system Part 11 compliant?	S:Yes	

4.3.2 Open System Questions

Reference	Question	Assessment Result	Remarks
11.30 Preamble references 94, 95, 96, 97	• Are there procedures and controls used to protect the authenticity and integrity of the electronic records from the point of their creation to the point of their receipt?	N/A	(see Q3 above)
	• As appropriate, are there procedures and controls used to protect the confidentiality of the electronic records from the point of their creation to the point of their receipt?	N/A	
	• Is document encryption (or an alternate technology) used to protect the confidentiality of the electronic records on the system?	N/A	
	• Are digital signatures (or an alternative technology) used to protect the authenticity and integrity of the electronic records on the system?	N/A	

4.3.3 Electronic Signature Questions

Reference	Question	Assessment Result	Remarks
Q6	• Does the system use any form of electronic signature that is intended to satisfy any regulatory or company requirement for a signature, initials, approval, authorization, etc.? If 'S:Yes", then check all that apply and continue with 11.10(j) - Biometric - Identification code and password - Identification code/password and Token If "No", skip the remaining questions. Be sure to differentiate between "signature" and "identification". If the intent is to use the applied identification to authenticate the electronic record, then the identification is an electronic signature. If the intent is to merely identify who did something, then the identification is not an electronic signature. A question to help determine if it's a "signature" or "identification" is "If I sign 'Jack Handy' , does that mean I have attested that I did or saw something, or that I'm authorizing some action?" If you have to sign the paper copy, you have to sign the electronic copy. Whether or not to use electronic signatures is not the system owner's choice. The choice is whether to use electronic records or not. That choice (plus the predicate rules) dictates whether electronic signatures are required or not.	S:Yes	Identification code and password as standard.

Reference	Question	Assessment Result	Remarks
Q6 (continued)	(A question to help determine if signatures are required is "If these were printed out, would you need to sign them?") … • Does the predicate rule require signatures on the record?	P:___	
	• Does company policy require signatures to be added to the record?	P:___	
	• Identify every display screen and report generated by the computerized system where an electronic signature is represented. Each occurrence should be separately assessed for compliance	P:___	
11.10(j) Preamble references 6, 88, 89, 90, 91	• Have written policies been established, and adhered to, that hold individuals accountable and responsible for actions initiated under their e-signatures in order to deter record and signature falsification?	P:___	
	• Is there a written procedure that describes user responsibilities for the use of computerized systems?	P:___	
	• Does it include not sharing passwords, periodically changing passwords, not using easy to guess passwords?	P:___	
	• Does it include not installing unapproved software and running virus protection software?	P:___	
	• Is there a **written** user acceptance/approval document that records their acknowledgement that their electronic signature is the legally binding equivalent of a handwritten signature?	P:___	

Reference	Question	Assessment Result	Remarks
11.50 Preamble references 98, 99, 100, 101, 102, 103, 104, 105, 106	• Do the signed electronic records contain the following information associated with the signing: 1. printed name of signer,	S:No	The user ID is stored. The printed name may not be unique over a network as the user ID is. The document, “Complying with 21 CFR Part 11 (Final Draft)” gives a contradictory annotation concerning the uniqueness of printed name and user ID.
	2. date and time that the signature was executed	S:Yes	
	3. the meaning associated with the signature?	S:No	The meaning is self–evident: creation of or amendment to a record.
	• Is the full name (first and last) displayed? The printed name cannot be the User ID.	S:No	See above. This requirement contradicts to the goal of unambiguity.
	• Is the meaning of the signature included?	S:No	See above. The meaning is self–evident.
	• Precision of time is based on risk. For example, the time might be reported in seconds for a data collection system. The time might be reported in minutes for a document management system.	S:Yes	The time is milliseconds.
	• Can the local time be derived if the system runs across time zones?	P:___	A procedural control must specify which time zone should be used in the PC, and keep track of possible changes.
	• Where is the time taken from? Is it protected from change by the user?	P:___	See comments above (section 11.10 e))
	• Are ad-hoc queries/reports allowed? If so, are there 4 components in the screen displays and reports?	S:Yes	The system administrator must configure templates for data output containing date/time and user ID of the author of a record.
	• Are these items subject to the same controls as for electronic records?	S:Yes	Templates are stored in a database and can be write-protected.
	• Are these items part of any human readable form of the electronic record?	S:Yes	If proper output templates are used. See above.

Reference	Question	Assessment Result	Remarks
11.70 Preamble references 107, 108, 109, 110, 111, 112, 113	• Is the electronic signature linked to their respective electronic record to ensure that the signature cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means?	S:Yes	
	• Is the transfer of the signature to another record prevented?	S:Yes	
	• Is the record protected to prevent changes after signing or to force re-signing?	S:Yes	
	• Are signature changes recorded in the audit trail?	N/A	
11.100 (a) Preamble references 16, 114, 115, 116	• Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	P:___	A procedural control must ensure that user ID's are never removed from the system but only made inactive if obsolete.
	• Does the system enforce unique username/id?	S:Yes	Windows NT or 2000 enforce unique user ID's over a network domain.
	• Is there a policy or procedure explicitly stating that each assigned electronic signature is unique to one person?	P:___	See above
	• Is there a policy or procedure that explicitly states that electronic signatures shall not be reused by or reassigned to anyone else?	P:___	
11.100(b) Preamble references 117, 118	• Are the identities of the individual verified prior to the establishment, assignment, and certification or otherwise sanctioning an individual's electronic signature or any element of an electronic signature ?	P:___	This is a standard task of the system administrator.
	• Has the contractor or temporary employee been cleared by Security or Human Resources to enter the workplace?	P:___	
	• Are controls in place to ensure that fake identities can be discerned with high reliability?	P:___	

Reference	Question	Assessment Result	Remarks
11.100(b) (continued) Preamble references 117, 118	• Are controls in place to verify that requestors are authorized to make requests for an e-signature (i.e., on behalf of themselves or another user)?	P:___	
	• Are individuals required to show id when they are given their electronic signatures/	P:___	
	• Are individuals requested to verify their identity if they forget their password?	P:___	
11.100(c) Preamble references 119, 120, 121	• Has the Company delivered its corporate electronic signature certification letter to FDA?	P:___	
	• Is it in paper form with a traditional handwritten signature?	P:___	
	• Can additional certification or testimony be provided that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature ?	P:___	
	• Is there documentation to support that individuals understand that electronic signatures are legally binding?	P:___	
	• What format is the additional testimony (training, signing of "evidence of understanding") in?	P:___	

4.3.4 Non-Biometric Signature Questions

Reference	Question	Assessment Result	Remarks
11.200(a) Preamble references 16,115,122 – 128 incl.	• Does the e-signature employ at least two distinct identification components such as User ID and password?	S:Yes	
	• When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all the electronic signature components?	S:Yes	
	• When an individual executes a series of signings during a single, continuous period of controlled system access, is each subsequent signing executed using at least one electronic signature component that is only executable by, and designed to be used by, the individual?	N/A	There is no series of signings.
	• When an individual executes one or more signings ***not*** performed during a single, continuous period of controlled system access, is each signing executed using all of the electronic signature components?	P:___	The system administrator must activate a password-protected screen saver to ensure that the user must log in again after a break.
	• Are the electronic signatures to be administered and executed to ensure that the attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals?	P:___	
	• Are the electronic signatures only to be used by their genuine owners?	P:___	
	• Initial log on to the system requires the execution of the identification code and password.	S:Yes	

Reference	Question	Assessment Result	Remarks
11.200(a) (continued) Preamble references 16,115,122 – 128 incl.	• The combination of these two components must be unique.	S:Yes	
	• The first signing requires both components.	S:Yes	
	• Is there a definition for a continuous session?	P:___	We propose to set a password-protected screen saver to a certain idle time.
	• Subsequent signings in the same session, requires only the password (which is the component known only to the signer)	P:___	
	• If, when resetting the account on some systems, a "default" password is assigned, is the user forced to change the password immediately upon log on?	P:___	
	• When an identification code and password are used as the electronic signature, is the password unknown to everyone, including the System Administrator?	P:___	
	• Are system tools used that might allow a System Administrator to falsify electronic records and/or electronic signatures? If so, are there procedures in place to ensure adequate controls over these activities?	P:___	
	• Does the system/workstation log-out after a period of inactivity?	P:___	
	• Do procedures and training reinforce that non-biometric electronic signatures must not be shared or loaned?	P:___	
	• Are safeguards in place that prevent one person from forging another person's electronic signature?	P:___	

4.3.5 ID Code and Password Only

Reference	Question	Assessment Result	Remarks
11.300(a)	• Are controls in place to ensure the uniqueness of each combined identification code and password maintained, such that no two individuals have the same combination of identification code and password?	P:___	Already covered in 11.100 (a)
	• Does a corporate policy exist?	P:___	
	• Is uniqueness maintained historically?	P:___	
	• Does the system check for duplicate Ids?	S:Yes	
11.300(b) Preamble reference 131	• Are controls in place to ensure that the identification code and password issuance is periodically checked, recalled, and revised?	P:___	
	• Does a corporate policy exist?	P:___	
	• Does the computerized system include functionality that requires users to periodically change their passwords (password aging)?	S:Yes	
	• Is there a manual procedure that requires users to periodically change their passwords?	P:___	
	• Is access periodically checked?	P:___	
11.300(d)	• Are transaction safeguards in use to prevent unauthorized use of passwords and/or identification codes?	S:Yes P:___	The system administrator must enable the proper policy of the operating system Windows NT or 2000 to fulfil this request.
	• Are transaction safeguards in use 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?	P:___	

Reference	Question	Assessment Result	Remarks
11.300(d) (continued)	• Is there a procedure or system function that revokes sign-on privileges when an incorrect combination of identification and password are repeatedly entered?	P:___	See above.
	• Has testing been conducted to ensure that "inactive" user accounts cannot be activated by unauthorized persons?	P:___	
	• Are there procedures and appropriate training to assure that users understand that passwords are not to be shared?	P:___	
	• Does the system create alert messages for unauthorized access attempts (e.g., access violations)?	P:___	
	• Is access frozen after a number of unsuccessful attempts to log in?	P:___	
	• Are "attempts at unauthorized use" defined?	P:___	
	• Are potential break-in attempts monitored in real-time?	P:___	
	• Is access violation reporting monitoring and escalation addressed in a SOP?	P:___	
	• Is "immediate and urgent" defined? Is the procedure and timing for notifying management defined?	P:___	
	• Does the procedure describe the security group's responsibility and required activities when notified of possible security breaches?	P:___	

4.3.6 ID Code/Password and Token Questions

Reference	Question	Assessment Result	Remarks
11.300(c) Preamble reference 132	• Are there loss management procedures in place to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information?	P:___	It is up to the pharmaceutical company to implement and/or use tokens or cards for access control. Sympatec is ready to supply such devices but the current standard is without.
	• Are there loss management procedures in place to issue temporary or permanent replacements using suitable, rigorous controls ?	P:___	
	• Does a corporate policy exist?	P:___	
	• Is there a procedure to describe how temporary replacements are handled?	P:___	
11.300(e) Preamble reference 138	• Are there controls in place to initially test devices that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner?	P:___	It is up to the pharmaceutical company to implement and/or use tokens or cards for access control. Sympatec is ready to supply such devices but the current standard is without.
	• Are there controls in place to periodically test devices that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner?	P:___	
	• Is there a procedure that requires both initial and periodic testing of these devices?	P:___	
	• Is initial testing of the devices conducted to ensure that they are tamper-proof and reliable?	P:___	

Reference	Question	Assessment Result	Remarks
11.300(e) (continued) Preamble reference 138	• Is periodic re-testing of devices conducted prior to putting new stock and/or models into service?	P:___	
	• Are there testing steps to ensure that devices operate within the manufacturer's operating parameters and functional tolerances?	P:___	

4.3.7 Biometric Signature Questions

Reference	Question	Assessment Result	Remarks
11.200(b) Preamble references 6,128	A properly designed and implemented biometric-based electronic signature system makes it unlikely that any electronic signature could be falsified.		It is up to the pharmaceutical company to implement and/or use biometric-based electronic signature systems (e.g. a fingerprint, a retinal pattern or a repeatable action like a handwritten signature) for access control. Sympatec is ready to supply such devices but the current standard is without.
	• Is the electronic signature designed to ensure that it cannot be used by anyone other than its true owner?	P:___	

4.4 Section J (Classification Section)

4.4.1 Applicability Sections of 21 CFR Part 11 (Closed System)

Scenario	Attributes	11.10	11.30	11.50	11.70	11.100	11.200(a)	11.200(b)	11.300 (a), (b), (d)	11.300 (c), (e)
1	Electronic Record Only (Closed System)	X								
2	Handwritten Signature Executed to Electronic Record (Hybrid)	X		X	X					
3	Electronic Signature Based upon Biometrics	X		X	X	X		X		
4	Electronic Signature Based upon ID Code/Password	X		X	X	X	X		X	
5	Electronic Signature Based upon ID Code/Password and Token	X		X	X	X	X		X	X

4.4.2 Classification Section

Scenario	Attributes	Sections which apply (Closed)	Sections which apply (Open)
1	Electronic Record Only (Closed System)	11.10 (except j)	11.10 (except j) 11.30
3	Handwritten Signature Executed to Electronic Record (Hybrid)	11.10 (except j) 11.50 11.70	11.10 (except j) 11.30 11.50 11.70
4	Electronic Signature Based upon Biometrics	11.10 11.50 11.70 11.100 11.200 (b)	11.10 11.30 11.50 11.70 11.100 11.200 (b)
5	Electronic Signature Based upon ID Code/Password	11.10 11.50 11.70 11.100 11.200 (a) 11.300 (a), (b), (d)	11.10 11.30 11.50 11.70 11.100 11.200 (a) 11.300 (a), (b), (d)
6	Electronic Signature Based upon ID Code/Password and Token	11.10 11.50 11.70 11.100 11.200 (a) 11.300 (c), (e)	11.10 11.50 11.70 11.100 11.200 (a) 11.300 (c), (e)

5 Support

If you need further support, please contact your local Sympatec After-Sales Service.