Siemens Opcenter
Siemens Opcenter Execution Pharma V6.2
Electronic Records / Electronic Signatures (ERES)
Compliance Response
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siemens Opcenter</td>
<td>1</td>
</tr>
<tr>
<td>Siemens Opcenter Execution Pharma V6.2</td>
<td>2</td>
</tr>
<tr>
<td>ERES Compliance Response</td>
<td>3</td>
</tr>
<tr>
<td>Product Information</td>
<td>4</td>
</tr>
</tbody>
</table>

Electronic Records / Electronic Signatures (ERES)

02/2020
A5E48761073-AA
Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

**DANGER**
indicates that death or severe personal injury will result if proper precautions are not taken.

**WARNING**
indicates that death or severe personal injury may result if proper precautions are not taken.

**CAUTION**
indicates that minor personal injury can result if proper precautions are not taken.

**NOTICE**
indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

**WARNING**
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.
Table of contents

1 Introduction...........................................................................................................................................5
2 The Requirements in Short...................................................................................................................7
3 Meeting the Requirements with Siemens Opcenter Execution Pharma............................................9
   3.1 Lifecycle and Validation of Computerized Systems ..............................................................9
   3.2 Suppliers and Service Providers ..............................................................................................9
   3.3 Data Integrity ...............................................................................................................................9
   3.4 Audit Trail, Change Control Support ..........................................................................................12
   3.5 System Access, Identification Codes and Passwords .............................................................13
   3.6 Electronic Signature .....................................................................................................................16
4 Evaluation List for Siemens Opcenter Execution Pharma.............................................................19
   4.1 Lifecycle and Validation of Computerized Systems ..............................................................19
   4.2 Suppliers and Service Providers ..............................................................................................21
   4.3 Data Integrity ...............................................................................................................................21
   4.4 Audit Trail, Change Control Support ..........................................................................................23
   4.5 System Access, Identification Codes and Passwords .............................................................23
   4.6 Electronic Signature .....................................................................................................................25
   4.7 Open Systems...............................................................................................................................27
Life science industry is basing key decisions on regulated records that are increasingly generated, processed and kept electronically. Reviews and approval of such data are also being provided electronically. Thus the appropriate management of electronic records and electronic signatures has become an important topic for the life science industry.

Accordingly, regulatory bodies defined criteria under which electronic records and electronic signatures will be considered as reliable and trustworthy as paper records and handwritten signatures executed on paper. These requirements have been set forth by the US FDA in 21 CFR Part 11 (21 CFR Part 11 Electronic Records; Electronic Signatures, US FDA, 1997; in short: Part 11) and by the European Commission in Annex 11 of the EU GMP Guideline (EU Guidelines to Good Manufacturing Practice, Volume 4, Annex 11: Computerised Systems, European Commission, 2011; in short: Annex 11).

Since requirements on electronic records and electronic signatures are always tied to a computerized system being in a validated state, both regulations also include stipulations on validation and lifecycle of the computerized system.

Application of Part 11 and Annex 11 (or their corresponding implementation in national legislation) is mandatory for the use of electronic records and electronic signatures. However, these regulations are only valid within their defined scope.

The scope of both regulations is defined by the regional market to which the finished pharmaceutical product is distributed and by whether or not the computerized systems and electronic records are used as part of GMP-regulated activities (see Part 11.1 and Annex 11 Principle).

Supplemental to the regulations, a number of guidance documents, good practice guides and interpretations have been published in recent years to support the implementation of the regulations. Some of them are referred to within this document.

To help its clients, Siemens as supplier of Siemens Opcenter Execution Pharma has evaluated version 6.2 of the system with regard to these requirements and published its results in this Compliance Response.

**Siemens Opcenter Execution Pharma V6.2 fully meets the functional requirements for the use of electronic records and electronic signatures.**

Operation in conformity with the regulations is ensured in conjunction with organizational measures and procedural controls to be established by the client (the regulated user). Such measures and controls are mentioned in chapter "Evaluation List for Siemens Opcenter Execution Pharma (Page 19)" of this document.
This document is divided into three parts:

1. Chapter "The Requirements in Short (Page 7)" provides a brief description of the requirement clusters.

2. Chapter "Meeting the Requirements with Siemens Opcenter Execution Pharma (Page 9)" introduces the functionality of Siemens Opcenter Execution Pharma V6.2 as means to meet those requirements.

3. Chapter "Evaluation List for Siemens Opcenter Execution Pharma (Page 19)" contains a detailed system assessment on the basis of the individual requirements of the relevant regulations.
Annex 11 and Part 11 take into account that the risk of manipulation, misinterpretation and changes without leaving a visible trace is higher with electronic records and electronic signatures than with conventional paper records and handwritten signatures. Furthermore the means to restrict access to electronic records to authorized individuals are very different to those required to restrict access to paper records. Additional measures are required for such reasons.

The terms "electronic record" / "electronic document" mean 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.

The term "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. Since electronic signatures are also considered as being electronic records by themselves, all requirements for electronic records are applied to electronic signatures too.

The following table provides an overview of the requirements from both regulations.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifecycle and Validation of Computerized Systems</td>
<td>Computerized systems used as a part of GMP-related activities must be validated. The validation process should be defined using a risk-based approach. It should cover all relevant steps of the lifecycle and must provide appropriate documented evidence. The system's functionality should be traceable throughout the lifecycle by being documented in specifications or a system description. A formal change control procedure as well as an incident management should be established. Periodic evaluation should confirm that the validated state of the system is being maintained.</td>
</tr>
<tr>
<td>Suppliers and Service Providers</td>
<td>Since competency and reliability of suppliers and service providers are considered key factors, the supplier assessment should be decided on a risk-based approach. Formal agreements should exist between the regulated user and these third parties, including clear responsibilities of the third party.</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Under the requirements of both regulations, electronic records and electronic signatures must be as reliable and trustworthy as paper records. The system must provide the ability to discern altered records. Built-in checks for the correct and secure handling of data should be provided for manually entered data as well as for data being electronically exchanged with other systems. The system's ability to generate accurate and complete copies is essential for the use of the electronic records for regulated purposes, as well as the accessibility, readability, and integrity of archived data throughout the retention period.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Audit Trail, Change Control Support</td>
<td>Besides recording changes to the system as defined in the lifecycle, both regulations require that changes on GMP-relevant data are being recorded. Such an audit trail should include information on the change (before / after data), the identity of the operator, a time stamp, as well as the reason for the change.</td>
</tr>
<tr>
<td>System Access, Identification Codes and Passwords</td>
<td>Access to the system must be limited to authorized individuals. Attention should be paid to password security. Changes on the configuration of user access management should be recorded. Periodic reviews should ensure the validity of identification codes. Procedures should exist for recalling access rights if a person leaves and for loss management. Special consideration should be given to the use of devices that bear or generate identification code or password information.</td>
</tr>
<tr>
<td>Electronic Signature</td>
<td>Regulations consider electronic signatures being legally binding and generally equivalent to handwritten signatures executed on paper. Beyond requirements on identification codes and passwords as stated above, electronic signatures must be unique to an individual. They must be linked to their respective electronic record and not be copied or otherwise being altered.</td>
</tr>
<tr>
<td>Open Systems</td>
<td>Open systems might require additional controls or measures to ensure data integrity and confidentiality.</td>
</tr>
</tbody>
</table>
The Siemens recommendations for the system architecture, conception and installation will assist system users in achieving compliance. For additional information and assistance, refer to Siemens Opcenter Execution Pharma functional and technical documentation from Siemens.

The requirements explained in chapter “The Requirements in Short (Page 7)” can be supported by the system as follows.

3.1 Lifecycle and Validation of Computerized Systems

In Annex 11 from 1992 and in Part 11 from 1997, the law already required that computerized systems need to be validated. Criteria for the validation of the system and its lifecycle were added in the edited revision of Annex 11 from 2011.

Nonetheless the requirements to validate a computerized system and to keep it in a validated state had long been a part of regulations other than Part 11 and Annex 11. This was the motivation for the ISPE (International Society of Pharmaceutical Engineers, http://www.ispe.org) to publish practical guidance like the Baseline Guides (Baseline® Pharmaceutical Engineering Guides for New and Renovated Facilities, Volume 1-7, ISPE), the GAMP 5 guide (GAMP 5 – A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE, 2008) as well as the GAMP Good Practice Guides.

Thus the system lifecycle as well as the approach to validation should be defined considering the guidance from the GAMP 5 guide. The guide also includes a number of appendices for lifecycle management, system development and operation of computerized systems. Since most pharmaceutical companies already have a validation methodology for computerized systems as a part of their process landscape, it is preferable to set up the systems lifecycle and validation according to these.

3.2 Suppliers and Service Providers

Suppliers of systems, solutions and services must be evaluated accordingly, see GAMP 5 Appendix M2. Siemens as a manufacturer of hardware and software components follows internal procedures of Product Lifecycle Management and works according to a Quality Management System, which is regularly reviewed and certified by an external certification company.

3.3 Data Integrity

Data integrity is assured in the system by measures like access protection, audit trail, data type checks, checksums, backup/restore, and archiving/retrieval, completed by system validation, appropriate procedures and training for personnel.
3.3 Data Integrity

Data storage

All data is stored in an Oracle database. As described in the security recommendation document it is strongly recommended to activate the advanced security functionality during installation of the database. Encryption of the database and the connection between server and client will therefore be enabled.

It is also possible to link external data, such as pdf files containing material certificates, to a data set. The responsibility for the integrity of all linked documents is in the regulated user.

Siemens Opcenter Execution Pharma can support the user by individually identifying each attached file and generating a checksum in order to detect any alteration to these documents. If an alteration is detected, the system will notify the user and display an error message.

Electronic batch report

Siemens Opcenter Execution Pharma is able to generate a clearly structured electronic batch report in PDF/A file format to allow easy review and archiving of the completed batch record. The electronic batch report contains a comprehensive summary and attachments with detailed information. These attachments consist of weighing and dispensing reports, the execution report which describes the batch manufacturing in detail and the annex collection. Additional necessary records may be created individually.

The electronic batch report may be generated either any time manually or at specific events automatically for example when the status of the batch review becomes approved. Siemens Opcenter Execution Pharma can then notify via email the successfully generation of the pdf file containing the electronic batch record.

Archiving

Siemens Opcenter Execution Pharma provides a configurable and scalable archiving function. Messages and measured values are stored continuously to the local database and external files are stored in a repository folder.

The stored data in the database can be transferred automatically to long-term archives. Archived data can be retrieved within the entire, configured retention period. Data can also be moved from the archive database to the export database, which is being used as an interface to third party archiving tools. External data needs to be handled accordingly to the archiving strategy of the regulated user and the Siemens Opcenter Execution Pharma functional documentation.
Set up screen: archiving strategy

Figure 3-1
3.4 Audit Trail, Change Control Support

"Audit trails are of particular importance in areas where operator actions generate, modify, or delete data in the course of normal operation." (Guidance for Industry Part 11 – Scope and Application, FDA, 2003)

An audit trail is not required for automatically generated electronic records which can neither be modified nor deleted by the operator. The system provides adequate system security mechanisms for such electronic records (e.g. access protection).

The following sections describe the implementation of requirements with regard to the audit trails during runtime operation and provide information on tracking changes made in the engineering system.

Audit trail

Siemens Opcenter Execution Pharma supports the requirement for audit trail of GMP relevant operations by recording such actions appropriately (who, what, when, and optionally why) and it provides adequate system security for such electronic records (e.g. access control). The GMP relevant data is defined by the regulated company based on the applicable regulatory requirements. All audit trails can either be printed on paper or be exported in an electronical format.

Operator actions performed in Siemens Opcenter Execution Pharma are being recorded in an audit trail containing information like old value, new value, user ID, date and time stamp, operation and optionally comments.
Changes made in user management

User management can be set up using Siemens Opcenter Execution Pharma authentication system or can be delegated to Microsoft Active Directory. If the Siemens Opcenter Execution Pharma authentication system is used all changes are subject to the audit trail. If Microsoft Active Directory is being used any changes made in the course phase of user management (e.g. setup of new users, blocking users, etc.) are recorded in the event log of Microsoft Windows. The event log must be configured accordingly, as described in the Microsoft documentation.

3.5 System Access, Identification Codes and Passwords

Users must be assigned the required access rights only, to prevent unauthorized access to the file system, the directory structures, and the system data and their unintended manipulation.

The requirements regarding access security are fully met in combination with procedural controls, such as those for "specifying the responsibility and access authorization of the system users".
Additional security mechanisms need to be set up for any “open paths” which might exist. For more information on the basic policies of the security concept and configuration recommendations, refer to the Siemens Opcenter Execution Pharma security manual.

The Siemens Opcenter Execution Pharma user management application, a basic functionality of Siemens Opcenter Execution Pharma, is used to set up user management either based on Microsoft Windows security mechanisms or as a standalone solution. The basic functionalities of this application are listed below:

- Management of the system functionalities
- Management of user groups
- Management of user accounts
- Modification of the current user's password
- Management of audit trail

Thereby the following requirements for access protection are fulfilled:

- Central user management (setup, deactivation, blocking, unblocking, assignment to user groups) by the administrator
- Use of a unique user identification (user ID) in combination with a password
- Definition of system functionalities and access for specific user groups
- Password settings and password aging: The user is forced to change his/her password on expiry of a time that is easily configured in the profile; the password can be reused only after “n” generations
- Prompt the user to define a new password at initial logon (initial password)
- The user is automatically blocked after a configurable number of failed logon attempts and can only be unblocked by administrators who have the user management rights
- Automatic lock after a configurable idle time of the keyboard and mouse or if the application is running during the idle time as a background task
- Log functions for actions related to access security, such as logon, manual and automatic logoff, input of incorrect user ID or password, user put into not allowed status after several attempts to enter an incorrect password, and password change by user
- Concurrent access in order to enter records is being prohibited by the system

In addition, users must be assigned specific access rights at operating system level to prevent unauthorized access to the directory structure of the Siemens Opcenter Execution Pharma system programs and unintended manipulation.

Figure 3-4 Assigning functions to the group weighing operator
3.6 Electronic Signature

Siemens Opcenter Execution Pharma provides functions for configuring an electronic signature. The operations or actions which require an electronic signature, which group is able to sign this action and the sequence of signatures are specified during the configuration phase. In order to meet the individual validation process, four different electronic signature types are predefined:

- Single electronic signature (signature of the user who performed the action)
- Double (conditional) electronic signature (if the original operator does not have the rights to validate the performed action an additional signature of a responsible user is needed)
- Single check electronic signature (signature of a user who differs from the user who performed the action)
- Double check electronic signature (signature of the user who performed the action and a user who did not perform the action)

Figure 3-5 Configuring electronic signature for different actions

The electronic signature is being executed in a separate dialog in which the user has to sign electronically by confirming the intended action with entering his password. Subsequently the electronic signature is saved in the audit trail along with the user name, time stamp, and the action performed. Also failed attempts to perform an electronic signature is saved in the audit.
A mandatory comment is needed to validate the electronic signature. Comments can be free text or predefined text for each electronic signature.

**Figure 3-6** Dialog double check electronic signature
3.6 Electronic Signature
The following list of requirements includes all regulatory requirements from 21 CFR Part 11 as well as from Annex 11 of the EU-GMP Guidelines. All requirements are structured in the same topics as those introduced in the chapter "The Requirements in Short (Page 7)" of this Compliance Response.

The requirements listed fully consider both regulations, regardless of whether technological or procedural controls or a combination of both are needed to fully comply with Part 11 and Annex 11.

The answers include, among other things, information about how the requirement is handled during the development of the product and which measures should be implemented during configuration and operation of the system. Furthermore, the answers include references to the product documentation for technical topics and to the GAMP 5 guide for procedural controls that are already considered in the guide.

### 4.1 Lifecycle and Validation of Computerized Systems

The fundamental requirement that a computerized system, used as a part of GMP related activities, must be validated is extended in the revision of Annex 11 from 2011 by requirements detailing expectations on a system’s lifecycle.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Reference</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.1 Risk management should be applied throughout the lifecycle of the computerized system.</td>
<td>Annex 11, 1</td>
<td>The R&amp;D process for Siemens software products incorporates risk management accordingly. During the validation of a customer-specific application risk management should be ensured by the regulated user.</td>
</tr>
<tr>
<td>4.1.2 Validation of a system ensures its accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</td>
<td>21 CFR 11.10 (a)</td>
<td>Yes, the development of the software product (COTS, see Annex 11, glossary) is under the control of the Siemens QMS and the Product Lifecycle Management process. The regulated user should take appropriate measures to validate the application (see Annex 11, glossary), as well as maintaining its validated state.</td>
</tr>
<tr>
<td>4.1.3 Validation documentation covers relevant steps of the lifecycle.</td>
<td>Annex 11, 4.1</td>
<td>The development process of the software product covers all relevant documents. The responsibility for the validation of the application (see Annex 11, glossary) is with the regulated user.</td>
</tr>
<tr>
<td>4.1.4 A process for the validation of bespoke or customized systems should be in place.</td>
<td>Annex 11, 4.6</td>
<td>The validation process for customer-specific applications is under the responsibility of the regulated user. Nonetheless Siemens is able to offer support regarding validation activities. Also as part of the standard software package are all test protocols which might be used in the validation activities.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Reference</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>4.1.5 Change management and deviation management are applied during the validation process.</td>
<td>Annex 11, 4.2</td>
<td>Yes, the R&amp;D process for the software product includes change management, deviation management and fault corrections. The regulated user should ensure appropriate change management and deviation management (see GAMP 5, appendices M8 and D5).</td>
</tr>
<tr>
<td>4.1.6 An up-to-date inventory of all relevant systems and their GMP functionality is available. For critical systems an up-to-date system description […] should be available.</td>
<td>Annex 11, 4.3</td>
<td>The regulated user should establish appropriate reporting, a system inventory as well as system descriptions (see GAMP 5, appendix D6).</td>
</tr>
<tr>
<td>4.1.7 User Requirements Specifications should describe required functions, be risk-based and be traceable throughout the lifecycle.</td>
<td>Annex 11, 4.4</td>
<td>Specification of requirements is part of the development process during product development. For the project-specific configuration, the regulated user should take into account the user requirements appropriately in system's lifecycle (see GAMP 5, appendix D1).</td>
</tr>
<tr>
<td>4.1.8 Evidence of appropriate test methods and test scenarios should be demonstrated.</td>
<td>Annex 11, 4.7</td>
<td>Ensuring the suitability of test methods and scenarios is an integral part of the Siemens product's R&amp;D process and test planning. The regulated user should be involved in the agreement of testing practice (see GAMP 5, appendix D5) for the application.</td>
</tr>
<tr>
<td>4.1.9 Appropriate controls should be used over system documentation. Such controls include the distribution of, access to, and use of system operation and maintenance documentation.</td>
<td>21 CFR 11.10 (k)</td>
<td>During the development of the product the product’s documentation is treated as being part of the product. Thus the documentation itself is under the control of the development process. The regulated user should establish appropriate procedural controls during development and operation of the production system (see GAMP 5, appendices M9 and D6).</td>
</tr>
<tr>
<td>4.1.10 A formal change control procedure for system documentation maintains a time sequenced record of changes.</td>
<td>21 CFR 11.10 (k)</td>
<td>During the development of the product changes are handled according to the development process. The regulated user should establish appropriate procedural controls during development and operation of the system (see GAMP 5, appendices M8 and O6).</td>
</tr>
<tr>
<td>4.1.11 Persons who develop, maintain, or use electronic record/electronic signature systems should have the education, training and experience to perform their assigned task.</td>
<td>21 CFR 11.10 (i)</td>
<td>Siemens’ processes do ensure that employees have according training for their tasks and that such training is properly documented. Furthermore Siemens offers a variety of training courses for users, administrators and support staff.</td>
</tr>
<tr>
<td>4.1.12 Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.</td>
<td>Annex 11, 11</td>
<td>The regulated user should establish appropriate procedural controls (see GAMP 5, appendices O3 and O8).</td>
</tr>
</tbody>
</table>
4.1.13 All incidents should be reported and assessed.
The Siemens Opcenter Execution portfolio offers functionalities to support reporting on different system levels. The regulated user should establish appropriate procedural controls (see GAMP 5, appendix O5).

4.1.14 For the availability of computerized systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown.
The regulated user should appropriately consider the system in his business continuity planning (see GAMP 5, appendix O10).

4.2 Suppliers and Service Providers
If the regulated user is partnering with third parties for planning, development, validation, operation and maintenance of a computerized system, then the competence and reliability of this partner should be considered utilizing a risk-based approach.

4.2.1 When third parties are used, formal agreements must exist between the manufacturer and any third parties.
The regulated user is responsible to establish formal agreements with suppliers and third parties.

4.2.2 The competency and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.
The regulated user should assess its suppliers accordingly (see GAMP 5, appendix M2).

4.2.3 The regulated user should ensure that the system has been developed in accordance with an appropriate Quality Management System.
The development of Siemens products follows the R&D process stipulated in the Siemens Quality Management System.

4.2.4 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.
The regulated user is responsible for the performance of such reviews.

4.2.5 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.
Matter and extent of the documentation affected by this requirement should be agreed upon by the regulated user and Siemens. The joint non-disclosure agreement should reflect this requirement accordingly.

4.3 Data Integrity
The main goal of both regulations is to define criteria under which electronic records and electronic signatures are as reliable and trustworthy as paper records. This requires a high degree of data integrity throughout the whole data retention period, including archiving and retrieval of relevant data.
## 4.3 Data Integrity

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Reference</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1 The system should provide the ability to discern invalid or altered records.</td>
<td>21 CFR 11.10 (a)</td>
<td>Yes. Based on the Oracle database security settings, access is only possible via Siemens Opcenter Execution Pharma. An entry in the audit trail will be generated for any operator action (for example, the operator changes set points / alarm thresholds / the monitoring mode or acknowledges alarms). All relevant changes are recorded including time stamp, user ID, old value and new value and comment. Unauthorized changes are prevented by the system through access control. A finalized electronic batch record and archived data can be accessed in read only mode and cannot be altered. The handling of external files which might be attached to data of Siemens Opcenter Execution Pharma is in the responsibility of the regulated user. It is possible to implement security functionalities within Siemens Opcenter Execution Pharma to ensure the integrity of external files.</td>
</tr>
<tr>
<td>4.3.2 For records supporting batch release, it should be possible to generate printouts indicating if any of the data has been changed since the original entry.</td>
<td>Annex 11, 8.2</td>
<td>Yes. Modification of data is recorded in the general audit trail and can be printed out in a report.</td>
</tr>
<tr>
<td>4.3.3 The system should provide the ability to generate accurate and complete copies of electronic records in both human readable and electronic form.</td>
<td>21 CFR 11.10 (b) Annex 11, 8.1</td>
<td>Yes. Accurate and complete copies can be generated either manually or automatically in electronic portable document formats like PDF/A or on paper.</td>
</tr>
<tr>
<td>4.3.4 Computerized systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data.</td>
<td>Annex 11, 5</td>
<td>Yes. The exchange of data is ensured via the gateway database. In this module a built-in data type check validates the correctness of incoming data.</td>
</tr>
<tr>
<td>4.3.5 For critical data entered manually, there should be an additional check on the accuracy of the data.</td>
<td>Annex 11, 6</td>
<td>The system has built-in plausibility checks for data entry. In addition, a multiple signature or operator dialog can be realized as an additional check.</td>
</tr>
<tr>
<td>4.3.6 Data should be secured by both physical and electronic means against damage.</td>
<td>Annex 11, 7.1</td>
<td>In addition to the system’s access security mechanisms, the regulated user should establish appropriate security means like physical access control, backup strategy, limited user access authorizations, regular checks on data readability, etc. Furthermore the data retention period should be determined by the regulated user and appropriately considered in the users processes (see GAMP 5, appendices O3, O4, O8, O9, O11 and O13).</td>
</tr>
<tr>
<td>4.3.7 Regular backups of all relevant data should be done.</td>
<td>Annex 11, 7.2</td>
<td>Yes. The regulated user should establish appropriate processes for backup and restore (see GAMP 5, appendix O9).</td>
</tr>
</tbody>
</table>
### 4.3.8
Electronic records must be readily retrievable throughout the records retention period.

Reference:
- 21 CFR 11.10 (c)
- Annex 11, 17

Answer:
Yes.
As stated above, procedural controls for backup/restore and archiving/retrieval should be established.

### 4.3.9
If the sequence of system steps or events is important, then appropriate operational system checks should be enforced.

Reference:
- 21 CFR 11.10 (f)

Answer:
Yes, for example allowances can be made for a specific sequence of operator actions by configuring the work order accordingly.

---

## 4.4 Audit Trail, Change Control Support

During operation, regulations require the recording of operator actions that may result in the generation of new relevant records or the alteration or deletion of existing records.

### 4.4.1
The system should create a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data, the reason should be documented.

Reference:
- 21 CFR 11.10 (e)
- Annex 11, 9

Answer:
Yes.
Changes during operation can be traced back by the system itself via audit trail and contain information with time stamp, user ID, old and new value and comment. The audit trail is secure within the system and cannot be changed by a user. It can be made available and also be exported in electronic portable document formats.

### 4.4.2
Management systems for data and documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

Reference:
- Annex 11, 12.4

Answer:
The requested information is part of the user management and audit trail functionality.

### 4.4.3
Changes to electronic records shall not obscure previously recorded information.

Reference:
- 21 CFR 11.10 (e)

Answer:
Yes.
Recorded information is not overwritten and is always available in the database.

### 4.4.4
The audit trail shall be retained for a period at least as long as that required for the subject electronic records.

Reference:
- 21 CFR 11.10 (e)
- Annex 11, 9

Answer:
Yes, this is technically feasible and must be considered in the archiving process (see GAMP 5, appendices O9 and O13).

### 4.4.5
The audit trail should be available for review and copying by regulatory agencies.

Reference:
- 21 CFR 11.10 (e)

Answer:
Yes, see also requirement 4.4.1.

---

## 4.5 System Access, Identification Codes and Passwords

Since access to a system must be restricted to authorized individuals and the uniqueness of electronic signatures also depends on the authenticity of user credentials, user access management is a vital set of requirements regarding the acceptance of electronic records and electronic signatures.
### 4.5 System Access, Identification Codes and Passwords

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Reference</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5.1 System access should be limited to authorized individuals.</td>
<td>21 CFR 11.10 (d) 21 CFR 11.10 (g) Annex 11, 12.1</td>
<td>Yes, system access via Siemens Opcenter Execution Pharma User Management is either based on the operating system’s user administration or configured within the Siemens Opcenter Execution Pharma itself. Functions are to be allocated with user groups in Siemens Opcenter Execution Pharma. In addition procedural controls should be established by the regulated user, as described in GAMP 5, appendix O11.</td>
</tr>
<tr>
<td>4.5.2 The extent of security controls depends on the criticality of the computerized system.</td>
<td>Annex 11, 12.2</td>
<td>System security is a key factor during design and development of Siemens products. Nonetheless, since system security highly depends on the operating environment of each IT-system, these aspects should be considered in security management (see GAMP 5, appendix O11). Recommendations and support is given by Siemens’ Industrial Security approach.</td>
</tr>
<tr>
<td>4.5.3 Creation, change, and cancellation of access authorizations should be recorded.</td>
<td>Annex 11, 12.3</td>
<td>Changes in the user access management are being recorded and should be subject to change control procedures.</td>
</tr>
<tr>
<td>4.5.4 If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals), does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals).</td>
<td>21 CFR 11.10 (h)</td>
<td>Yes. The Siemens Opcenter Execution Pharma work center (workstations) can be configured so that special input data / commands can only be performed from a dedicated work center. All other work centers then have read only access rights at the most.</td>
</tr>
<tr>
<td>4.5.5 Controls should be in place to maintain the uniqueness of each combined identification code and password, so that no individual can have the same combination of identification code and password as any other.</td>
<td>21 CFR 11.300 (a)</td>
<td>Yes. If the user administration of the operating system is used as a platform for access management it is not possible to define more than one user with the same user ID within a workgroup / domain. If the user management of Siemens Opcenter Execution Pharma is used for access management it is not possible to define more than one user with the same short name, full name or initials. Thus each combination of user ID and password is unique.</td>
</tr>
<tr>
<td>4.5.6 Procedures are in place to ensure that the validity of identification codes is checked periodically.</td>
<td>21 CFR 11.300 (b)</td>
<td>The regulated user should establish appropriate procedural controls (see “Good Practice and Compliance for Electronic Records and Signatures, Part 2”).</td>
</tr>
<tr>
<td>4.5.7 Passwords should periodically expire and have to be revised.</td>
<td>21 CFR 11.300 (b)</td>
<td>Yes. Password aging is either based on the operating system’s user administration or on Siemens Opcenter Execution Pharma user management.</td>
</tr>
</tbody>
</table>
### 4.6 Electronic Signature

To ensure that electronic signatures are generally accepted as equivalent to handwritten signatures executed on paper, requirements are not only limited to the act of electronically signing records. They also include requirements on record keeping as well as on the manifestation of the electronic signature.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Reference</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5.8 A procedure should be established for recalling identification codes and passwords if a person leaves or is transferred.</td>
<td>21 CFR 11.300 (b)</td>
<td>The regulated user should establish appropriate procedural controls (see &quot;Good Practice and Compliance for Electronic Records and Signatures, Part 2&quot;). The Microsoft Windows security system can be used to deactivate user accounts. In the Siemens Opcenter Execution Pharma user management the corresponding user has to be put in the &quot;not allowed&quot; status.</td>
</tr>
<tr>
<td>4.5.9 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.</td>
<td>21 CFR 11.300 (c)</td>
<td>The regulated user should establish appropriate procedural controls (see &quot;Good Practice and Compliance for Electronic Records and Signatures, Part 2&quot;).</td>
</tr>
<tr>
<td>4.5.10 Measures for detecting attempts of unauthorized use and for informing security and management should be in place.</td>
<td>21 CFR 11.300 (d)</td>
<td>Yes, unsuccessful attempts to use the system or to perform electronic signatures are recognized and are logged. The regulated user should establish appropriate procedural controls to ensure a periodic review of security and access control information logs (see GAMP 5, appendix O8).</td>
</tr>
<tr>
<td>4.5.11 Initial and periodic testing of devices, such as tokens and 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.</td>
<td>21 CFR 11.300 (e)</td>
<td>Such devices are not part of the Siemens Opcenter Execution Pharma portfolio. The regulated user should establish appropriate procedural controls (see &quot;Good Practice and Compliance for Electronic Records and Signatures, Part 2&quot;).</td>
</tr>
<tr>
<td>Requirement</td>
<td>Reference</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>4.6.1 Written policies should be established that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.</td>
<td>21 CFR 11.10 (j) Annex 11, 14.a</td>
<td>The regulated user should establish appropriate procedural controls.</td>
</tr>
<tr>
<td>4.6.2 Signed electronic records should contain the following related information:</td>
<td>21 CFR 11.50 (a) Annex 11, 14.c</td>
<td>Yes.</td>
</tr>
<tr>
<td>● The printed name of the signer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● The date and time of signing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● The meaning of the signing (such as approval, review, responsibility)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.6.3 The above-listed information is shown on displayed and printed copies of the electronic record.</td>
<td>21 CFR 11.50 (b)</td>
<td>Yes.</td>
</tr>
<tr>
<td>4.6.4 Electronic signatures 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.</td>
<td>21 CFR 11.70 Annex 11, 14.b</td>
<td>Yes.</td>
</tr>
<tr>
<td>4.6.5 Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</td>
<td>21 CFR 11.100 (a) 21 CFR 11.200 (a) (2)</td>
<td>Yes, the electronic signature uses the unique identifiers for user accounts in the Microsoft Windows user administration or is locally defined in the Siemens Opcenter Execution Pharma user management. The re-use or re-assignment of electronic signatures is effectively prevented.</td>
</tr>
<tr>
<td>4.6.6 When a system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batch.</td>
<td>Annex 11, 15</td>
<td>Electronic signatures are linked to an individual and each individual is allocated to a group. The system allows strict determinations about which functions a group is allowed to perform a signature.</td>
</tr>
<tr>
<td>4.6.7 The identity of an individual should be verified before electronic signature components are allocated.</td>
<td>21 CFR 11.100 (b)</td>
<td>The regulated user should establish appropriate procedural controls for the verification of an individual’s identity before allocating a user account and or electronic signatures.</td>
</tr>
<tr>
<td>4.6.8 When an individual executes one or more signings not performed during a single session, each signing shall be executed using all of the electronic signature components.</td>
<td>21 CFR 11.200 (a) (1) (ii)</td>
<td>Yes, performing an electronic signature requires the user ID as well as the user’s password.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Reference</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>4.6.9 When an individual executes a series of signings during a single session, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one private electronic signature component.</td>
<td>21 CFR 11.200 (a) (1) (i)</td>
<td>Yes. Each signature consists of two components (user ID and password).</td>
</tr>
<tr>
<td>4.6.10 The use of an individual's electronic signature by anyone other than the genuine owner would require the collaboration of two or more individuals.</td>
<td>21 CFR 11.200 (a) (3)</td>
<td>Yes. It is not possible to falsify an electronic signature during signing or after recording of the signature. In addition, the regulated user needs procedures that prevent the disclosure of passwords.</td>
</tr>
<tr>
<td>4.6.11 Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owner.</td>
<td>21 CFR 11.200 (b)</td>
<td>Standard tools of third party manufacturers can be used to create biometric electronic signatures. The integrity of such solutions should be assessed separately.</td>
</tr>
</tbody>
</table>

### 4.7 Open Systems

The operation of an open system may require additional controls to ensure data integrity as well as the possible confidentiality of electronic records.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Reference</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7.1 To ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records additional measures such as data encryption are used.</td>
<td>21 CFR 11.30</td>
<td>All communications are performed via SSL encryption. Detailed information about security measures are described in the security manual.</td>
</tr>
<tr>
<td>4.7.2 To ensure the authenticity and integrity of electronic signatures, additional measures such as the use of digital signature standards are used.</td>
<td>21 CFR 11.30</td>
<td>Siemens Opcenter Execution Pharma does not provide functionality for digital (encrypted) signatures.</td>
</tr>
</tbody>
</table>