
Standard Operating Procedure

21 CFR Part 11 - Scope and Controls



This is an example of a Standard Operating Procedure. It is a proposal and starting point only. The type and extent of documentation depends on the process environment. The proposed documentation should be adapted accordingly and should be based on individual risk assessments. There is no guarantee that this document will pass a regulatory inspection.

Publication from www.labcompliance.com

Global on-line resource for validation and compliance

Copyright by Labcompliance. This document may only be saved and viewed or printed for personal use. Users may not transmit or duplicate this document in whole or in part, in any medium. Additional copies and licenses for department, site or corporate use can be ordered from www.labcompliance.com/solutions.

While every effort has been made to ensure the accuracy of information contained in this document, Labcompliance accepts no responsibility for errors or omissions. No liability can be accepted in any way.

Labcompliance offers books, master plans, complete Quality Packages with validation procedures, scripts and examples, SOPs, publications, training and presentation material, user club membership with more than 250 downloads and audio/web seminars. For more information and ordering, visit www.labcompliance.com/solutions

Company Name:	
----------------------	---

Controls:	
Superseded Document	N/A, new
Reason for Revision	N/A
Effective Date	Jan 1, 2004

Signatures:	
Author	<p>I indicate that I have authored or updated this SOP according to applicable business requirements and our company procedure: Preparing and Updating Standard Operating Procedures.</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Date: _____</p>
Approver	<p>I indicate that I have reviewed this SOP, and find it meets all applicable business requirements and that it reflects the procedure described. I approve it for use.</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Date: _____</p>
Reviewer	<p>I indicate that I have reviewed this SOP and find that it meets all applicable quality requirements and company standards. I approve it for use.</p> <p>Name: _____</p> <p>Signature: _____</p> <p>Date: _____</p>

1. PURPOSE

In March of 1997 the FDA issued final Part 11 regulations that provide criteria for acceptance by the FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. After Part 11 became effective in August 1997, significant discussions ensued among industry, contractors, and the Agency concerning the interpretation and implementation of the regulations. While initial FDA guidance documents indicated a very broad scope with significant problems to fully implement Part 11, in 2003 the FDA released a new guidance promoting a more narrow scope. This SOP should help to implement Part 11 requirements in the most cost effective way.

2. SCOPE

The SOP applies to electronic records in GxP environments and to other records, such as paper or microfiche that originated from electronic records. The SOP reflects the FDA's approach for scope and application of 21 CFR Part 11 according to Reference 4.2. Currently the FDA is reexamining Part 11 and plans to initiate a new rule. When the new rule is released, the content of this SOP should be re-evaluated and updated for compliance with the new rule.

3. GLOSSARY/DEFINITIONS

Item	Explanation
GxP	Good x Practices where x can stand for L=Laboratories, M=Manufacturing, C=Clinical
Electronic Record	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.
Electronic Signature	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.
Handwritten Signature	The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention

	to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
Predicate Rule	Requirements set forth in the Public Health and Safety (PHS) Act, or any FDA regulation, with the exception of Part 11. Examples are Good Laboratory Practice, Good Manufacturing Practice and Good Clinical Practice Regulations.
GxP Record	Record required to be maintained by predicate rules or submitted to the FDA under the predicate rules.
Closed System	An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
Open System	An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.
Regulated Activity	Any activity required by a predicate rule.
Original Record	Electronic records originally captured by the computer system. This can be a manual data entry or a record captured from an automated system. When records are converted to a standard format, e.g., an original word document to PDF format, these are no longer original formats.

Note: For other definitions, see www.labcompliance.com/glossary.

4. REFERENCE DOCUMENTS

- 4.1. Code of Federal Regulations, Title 21, Food and Drugs, Part 11 Electronic Records; Electronic Signatures; Final Rule; Federal Register 62 (54), 13429-13466.
- 4.2. FDA Guidance for Industry Part 11, Electronic Records; Electronic Signatures Scope and Applications (Final version August 2003).
- 4.3. SOP ##### "Risk Assessment for Systems Used in GxP Environments".
- 4.4. SOP ##### "Risk-Based Validation of Computer Systems".

4.5. SOP ##### "Retention of GxP Records".

5. RESPONSIBILITIES

5.1. System Owner

5.1.1. Owns the process for defining and documenting scope and controls for records created, modified, maintained, archived, retrieved, or distributed by a computer system.

5.1.2. Drafts documentation.

5.2. Operation's Manager

5.2.1. Gives inputs on business practices.

5.2.2. Reviews and approves documentation for compliance with business practices.

5.3. Quality Assurance

5.3.1. Advises on regulations and guidelines related to 21 CFR Part 11.

5.3.2. Reviews documentation for compliance with the company's definition of Part 11 scope and controls.

5.3.3. Reviews the processes and documentation for compliance with other internal policies and regulations/guidelines.

5.3.4. Approves documentation.

6. FREQUENCY OF USE

6.1. Initially whenever the Part 11 scope and controls are defined.

6.2. After system updates or other changes and when the change indicates that the Part 11 scope and controls may need to be changed.

6.3. Whenever system reviews indicate that the Part 11 scope and controls may need to be changed.

7. PROCEDURE

7.1. Overview

The process for defining scope and controls is explained in Figure 1. It requires a thorough documentation of the business practices and good knowledge of predicate rule requirements.

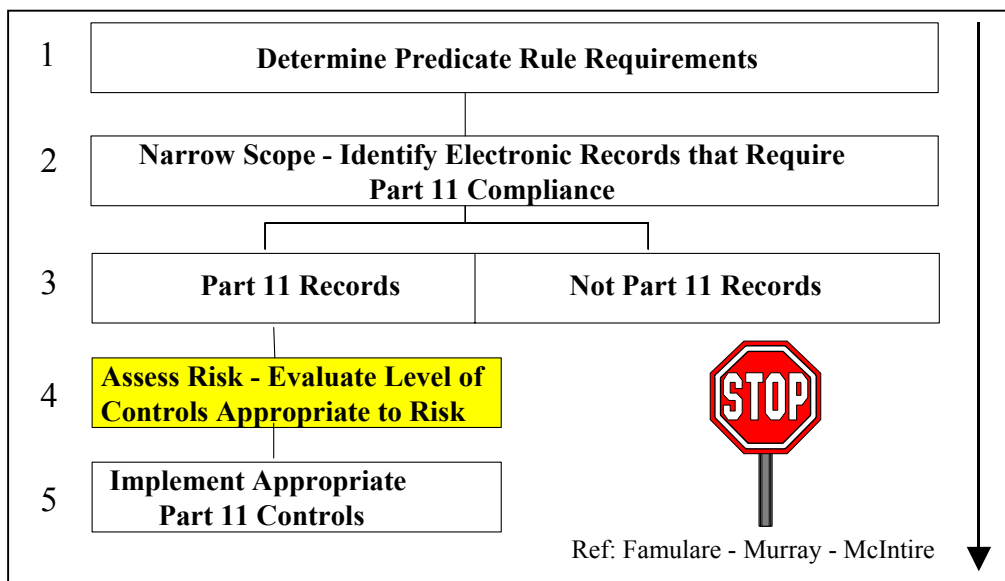


Figure 1. Flow Chart to Define Scope and Controls for Part 11

First we check if the record is required by the predicate rule or submitted to the FDA. Next, we determine if the record fits in with the new, narrow scope of Part 11. The main criterion is whether the record is maintained in electronic format in place of paper format, or if the original electronic record is converted to another format, either paper or a standard electronic format, and persons rely on the electronic record to perform regulated activities. Finally, we make a risk assessment of the criticality of the Part 11 records and document the result. Based on the outcome appropriate Part 11 controls are implemented.

7.2. Documentation of the Business Practices

- 7.2.1. The system owner collects inputs on business practices. Information can come from staff and management of the operational department and/or from existing documentation such as SOPs. Inputs should include:
- 7.2.1.1. Practices to create, modify, maintain, archive, retrieve or distribute records.
 - 7.2.1.2. Information on who has access to the system and records and when.
 - 7.2.1.3. Information on if and how users who have access to the system can manipulate records.
 - 7.2.1.4. Information on if and how the manipulated records can impact the quality of products.
 - 7.2.1.5. Information on who signs what and in which format (electronic signatures vs. handwritten signatures).
- 7.2.2. Using information from 7.2.1 the system owner documents the business practices. For complex processes documentation should be supported by graphics. The example in Attachment 8.1 can be used as a template.

7.3. Assessment and Documentation if GxP Records are Generated

- 7.3.1. The system owner evaluates if any of the created, modified, maintained, archived, retrieved, or distributed records are required to be maintained by a predicate rule and/or are submitted to the FDA in electronic form. Note: A record that is not itself submitted, but is used in generating a submission, is not a Part 11 record unless it is otherwise required to be maintained under a predicate rule and it is maintained in electronic format.
- 7.3.2. The findings of 7.3.1 are then documented. If there is no predicate rule requirement for the records and the records are not submitted to the FDA in electronic form the process is stopped. If there is a predicate rule requirement to maintain the records, reference to the predicate rule is documented. Note: Requirements should be classified into explicit requirements and implicit requirements. Explicit are those records that are spelled out by the rule, implicit records are not spelled out as a record requirement but should be available to document a predicate rule requirement. An example for implicit requirements are training records for drug GMPs.

7.3.3. If the business practices indicate that the records are signed electronically and maintained only in electronic form, proceed to Section 7.5. Otherwise continue with 7.4.

7.4. Assess if Persons Rely on Records in Electronic Form to Perform Regulated Activities

7.4.1. The system owner checks with operators to find out if any persons rely on records in electronic form to perform regulated activities. An example would be if the function of the computer can influence a regulated activity, for example, a laboratory test result that will have an impact on whether a drug product is released or not.

7.4.2. The system owner documents the outcome of 7.4.1. If nobody relies on the electronic records to perform regulated activities, stop the process.

7.5. Perform and Document Risk Assessment

7.5.1. The system owner initiates a risk assessment following the SOP ####: "Risk Assessment for Systems Used in GxP Environments".

7.5.2. The system owner documents the outcome of the risk assessment.

7.6. Implementing Part 11 Controls

7.6.1. Controls to be implemented for all Part 11 records:

7.6.1.1. Limiting system access to authorized individuals.

7.6.1.2. Use of operational system checks.

7.6.1.3. Use of authority checks.

7.6.1.4. Use of device checks.

7.6.1.5. Confirmation that the people who develop, maintain or use electronic systems have the education, training and experience to perform their assigned tasks.

7.6.1.6. Establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures.

7.6.1.7. Appropriate controls over systems documentation.

7.6.1.8. Binding signatures to records for open and closed signatures.

7.6.1.9. Use of digital signatures for open systems.

7.6.2. Validation

Validation of computer systems used in GxP environments is a requirement of all predicate rules and therefore all systems used in such environments should be validated. However, the extent of validation depends on the risk the system has on product quality, safety and record integrity. For example, a computerized analytical system used in a QC laboratory requires full validation with OQ tests like stress testing, boundary testing and life testing. On the other hand a good documentation of installation and change control procedures is sufficient for word processing systems used to generate validation reports or SOPs.

7.6.2.1. Validate the system using criteria from Reference 4.4.

7.6.3. Electronic Audit Trail

7.6.3.1. An electronic audit trail is required if audit trail is a requirement of the predicate rule and all criteria from 7.6.3.1.1 to 7.6.3.1.3 apply.

7.6.3.1.1. Systems/records are classified as medium or high risk.

7.6.3.1.2. Operators can manipulate electronic records during normal operation.

7.6.3.1.3. Manipulated records can have a negative impact on product quality or safety and record integrity.

7.6.3.2. If audit trail is a requirement of a predicate rule and one of the criteria from 7.6.3.1.1 to 7.6.3.1.3 does not apply and electronic audit trail is not implemented, manual audit trail must be implemented.

7.6.3.3. Even if there are no predicate rule requirements to document, for example, date, time or sequence of events in a particular instance, it may nonetheless be important to have audit trails or other physical, logical or procedural security measures in place to ensure the trustworthiness and reliability of the records.

7.6.4. Copies of Records

7.6.4.1. When copying original records to other electronic formats or to other non-electronic formats the copying process used to produce

the copies should preserve the content and meaning of the record.

7.6.4.2. Electronic records should be made available to inspectors in the same way as they are available to users in the department. For example:

7.6.4.2.1. If you have the ability to search, sort or trend Part 11 records, copies given to the Agency should provide the same capability if this is reasonable and technically feasible.

7.6.4.2.2. You should allow inspection, review and copying of records in a human readable form at your site using your hardware and following your established procedures and techniques for accessing records.

Note: Copies of electronic records from the computer system should be given to the inspector to take away if requested, but you cannot give away software for evaluation from the computer system.

7.6.5. Record Retention

7.6.5.1. Retention and maintenance of records, e.g., availability and duration, should comply with all applicable predicate rule requirements and with the SOP #####: "Retention of GxP Records".

7.6.5.2. Records should be maintained and archived in original electronic form if the record/system is classified as high or medium risk and if one of the criteria from 7.6.5.2.1 and 7.6.5.2.2 applies:

7.6.5.2.1. The records provide a high value and are available to the department for further evaluation or reevaluation.

7.6.5.2.2. The copying process to other formats does not preserve the original content. An example would be if metadata required demonstrating the record's integrity and/or predicate rule requirements cannot be copied.

7.6.5.3. For systems classified as low risk or if none of the criteria from 7.6.5.2.1 to 7.6.5.2.2 apply, records can be converted to non-electronic media such as microfilm, microfiche and paper, or to a standard electronic file format (examples of such formats include, but are not limited to, PDF, XML or SGML). You must still comply

with all predicate rule requirements, and the records themselves and any copies of the required records should preserve their content and meaning. As long as predicate rule requirements are fully satisfied and the content and meaning of the records are preserved and archived in other formats, you can delete the original electronic version of the records.

7.6.6. Legacy Systems

7.6.6.1. For legacy systems classified as high-risk systems implement the same controls as for “non-legacy” systems.

7.6.6.2. If the system lacks Part 11 controls, develop a gap analysis and remediation plan.

7.6.6.3. For medium-risk systems check 7.6.6.3.1 to 7.6.6.3.6. If the answer to one of the questions is “no”, Part 11 controls should be implemented as for a non-legacy system.

7.6.6.3.1. Was it operational prior to August 20th, 1997?

7.6.6.3.2. Did it meet all applicable predicate rules before August 20th, 1997?

7.6.6.3.3. Is there documented evidence of this?

7.6.6.3.4. Has the system changed since August 20th, 1997 and has the impact of the change been formally evaluated and documented and was the outcome of the evaluation that the changed system still complied with predicate rule requirements?

7.6.6.3.5. Are key functions still the same as on August 20th, 1997 and no new functions have been added that could impact the integrity and accuracy of electronic records?

7.6.6.3.6. Is there an acceptable level of record security and integrity?

7.7. Review and Approval

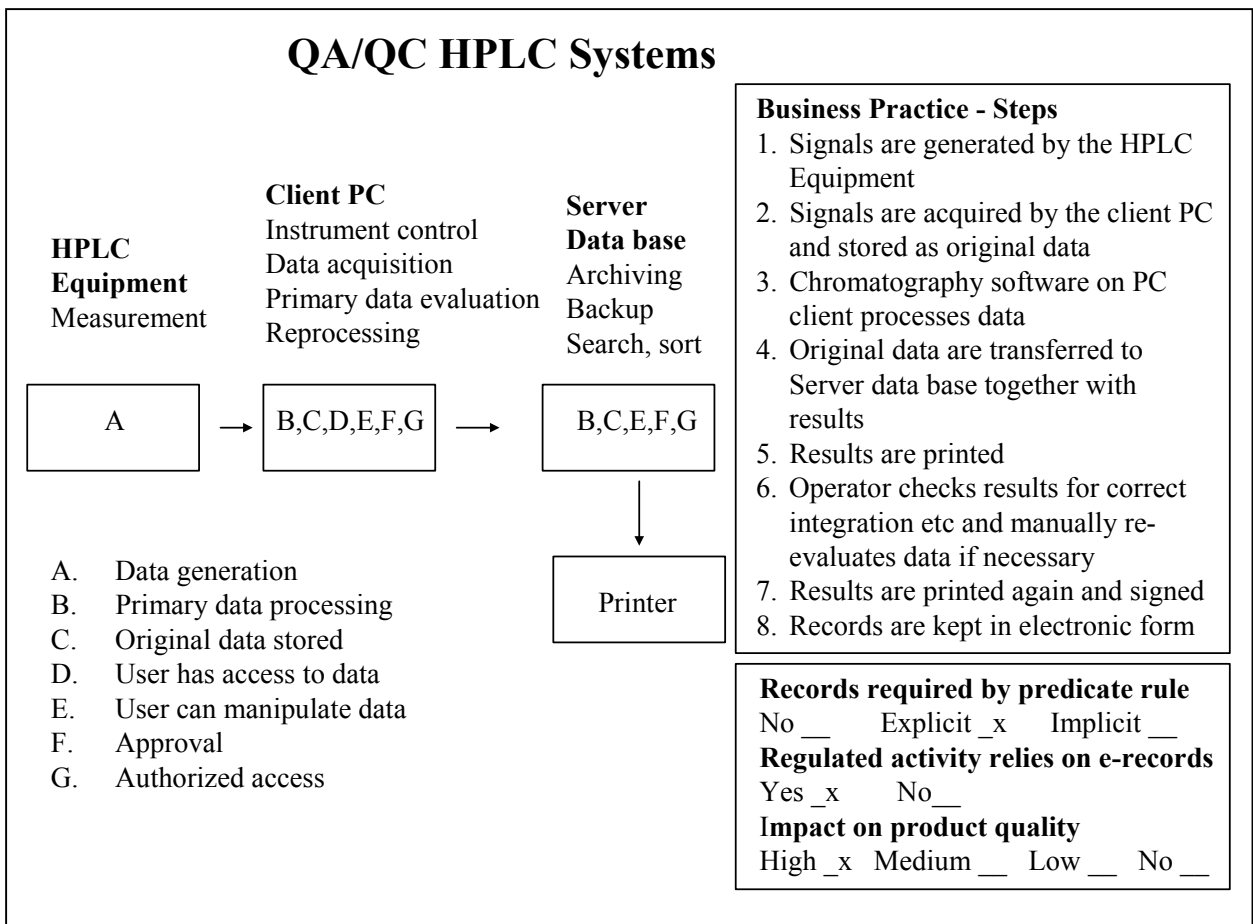
7.7.1. The documents as developed in Sections 7.2 to 7.6 are reviewed and approved by the operation’s manager for compliance with business practices.

7.7.2. The documents as developed in sections 7.2 to 7.6 are reviewed and approved by the QA management for compliance with regulations and internal standards and guidelines.

8. ATTACHMENTS

8.1. Attachment – Example for Documentation of Business Practices

A graphics or presentation software package can be used to document the graphic portion.



8.2. Attachment – Documenting Part 11 Controls

QA/QC HPLC System	
GxP records?	Yes. GMP - Laboratory results.
Do people rely on e-records to perform regulated activities?	Yes. Accuracy of laboratory results is largely influenced by correct functioning of the computer software.
Legacy system? Check 7.6.6	No. In 1997 the system was upgraded from a stand-alone computer system to a client server networked data system with a significant new functionality.
Part 11 records?	Yes
Controls (not under enforcement discretion):	Limited system access to authorized individuals. Operational system checks. Device checks. People training/qualification. People accountability for e-signatures. Controls over system documentation. Controls for open systems.
Validation: Check 7.6.2	System should be validated following SOP #####: "Risk-Based Validation of Computer Systems".
Electronic Audit Trail: Check 7.6.3	Electronic audit trail should be implemented. <ul style="list-style-type: none"> • Operators can manipulate electronic records during normal operation. • Manipulated records can have a negative impact on product quality or safety and record integrity.
Copies of E-records: Check 7.6.4	Copies should be available in electronic form. <ul style="list-style-type: none"> • Original records, metadata and processed data are available in the laboratory for reprocessing, database search and sort.
Record Retention: Check 7.6.5	Original records, meta data and processed records should be maintained and archived in original electronic form. <ul style="list-style-type: none"> • The records provide a high value and are available to the department for further evaluation or reevaluation • Copying process to other formats does not fully preserve the original content.