GAMP
SPECIAL INTEREST GROUP
(21 CFR Part 11)

Complying with 21 CFR Part 11
Electronic Records and Electronic Signatures

Final Draft

01 September 2000

Document Ref: GAMP/SIG/21 CFR Part 11
Issue: Final Draft
Author: GAMP 21 CFR Part 11 Special Interest Group

Copy No:

COMPANY CONFIDENTIAL

This document contains 87 pages.

PREFACE

UNDER REVIEW

Document History

First Draft (internal)	November 1999	Made available internally to GAMP SIG for comment.
First Draft	December 1999	Made available to GAMP Forum, ISPE, & PDA for comment
Final Draft	July 2000	Made available to industry and regulators for comment

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

The FDA rule relating to the use of Electronic Records and Electronic Signatures (21 CFR Part 11) is one of the most significant pieces of new legislation to affect the pharmaceutical manufacturing industry in recent times.

With ever greater use of information technology and computer systems at all stages of manufacture, more and more of the operating processes are being automated. As a result, key decisions and actions are being taken through electronic interfaces, with regulatory records being generated electronically.

For the first time, 21 CFR Part 11 introduces specific controls on the use of electronic records and includes strict administrative controls on electronic signatures. In practice, these will impose an administrative burden over and above that previously considered good practice in most companies.

FDA's view is that the risks of falsification, misinterpretation, and change without leaving evidence are higher with electronic records than paper records, and that therefore specific controls are required. See quotation below from Preamble to Final Rule, *Comments on the Proposed Rule*, Section F.

"...people determined to falsify records may find a means to do so despite whatever technology or preventive measures are in place. The controls in part 11 are intended to deter such actions, make it difficult to execute falsification by mishap or casual misdeed, and to help detect such alterations when they occur."

Current FDA thinking is now becoming visible as a result of recently published warning letters (see Appendix 8), and on-going dialogue with industry.

Despite the number of controls, the FDA rule on Electronic Records and Electronic Signatures is one of the few pieces of compliance legislation that the industry sought to enable the use of advances in technology. 21 CFR Part 11 allows hand-written signatures to be substituted by electronic alternatives, for manufacturing and regulatory documentation (unless paper-based records are a specific requirement in existing regulations that pertain to the records themselves). Within the GMP environment an immediate benefit is the legalising of the use of electronic batch recording and production records, laboratory information management systems, electronic laboratory notebooks, fully automated production of Certificates of Analysis and many more applications within the manufacture of pharmaceutical products. Another obvious advantage is the acceptability of electronic submissions in the areas of new drug applications and updates.

Whilst recognising the long-term benefits 21 CFR Part 11 will bring in permitting technological advances, industry is also faced with applying the rule to existing systems (sometimes referred to as legacy systems) and current projects. With this comes an urgent need to improve understanding of the rule, its interpretation, and application.

This document has been produced by a Special Interest Group of the GAMP Forum, under the chairmanship of Dr Tony Margetts (AstraZeneca Pharmaceuticals), in order to promote a better understanding of 21 CFR Part 11. It aims to provide industry with practical guidance on how to comply with the rule, while highlighting and addressing common issues of concern.

The document is structured as follows:

- **Objectives** – Purpose and aim of this document.

- **Scope –** When, and to whom, this document applies.

- **Management Approach –** Description of a management process for pharmaceutical companies to achieve and maintain compliance with 21 CFR Part 11. Specific guidance is provided for both new and existing systems. The role of suppliers in supporting this approach is also highlighted.

- **Conclusions**

- **Appendices –** Information, examples, templates, and checklists to use when implementing 21 CFR Part 11 compliance programmes. Also, related Glossary and References List.

1.2 GAMP FORUM

The GAMP Forum was established in 1991 to help promote the understanding of how computer systems validation should be carried out in the pharmaceutical industry. It did this by developing a guide to validation taking input from not only the industry, but also from its suppliers and the regulators, particularly the Medicines Control Agency in the UK.

The first draft was issued for comment in 1994 and since then three subsequent revisions have been published as "The GAMP Guide to Computer and Automated Systems Validation". Each addition has built on previous versions adding details of best practice as they evolve.

The GAMP Forum, with its focus to-date on the application of GMP to the information technology environment generally, continues to work in areas of current relevance to the industry. In August 1997, a new regulation from the FDA was introduced, 21 CFR Part 11 entitled "Electronic Records; Electronic Signatures". The proposed interpretative guidance in this draft document has been developed as part of the continuing efforts of the GAMP Forum to provide a mechanism for the industry, its suppliers, and regulators together to develop and document best practice in this specific area.

1.3 ACKNOWLEDGEMENTS

This document was produced by the GAMP Forum Electronic Records and Signatures Special Interest Group between July and November 1999.

Tony Margetts (AstraZeneca, Chairman)
Paul Grey (AstraZeneca)
Colin Jones (Mi Services Group)
Leif Poulsen (Novo Nordisk)
Peter Robertson (AstraZeneca)
David Selby (Selby Hope International).
Caroline Smith (BASF Pharma)
Anthony J.Trill (Medicines Control Agency)
Peter Wilks (GlaxoWellcome)
Guy Wingate (GlaxoWellcome)
Sion Wyn (Mi Services Group))

The initial draft of this document was technically authored by David Selby, Tony Margetts, and Colin Jones. Their diligence is gratefully acknowledged.

The document was revised and updated during July 2000 by Tony Margetts and Colin Jones following feedback on the first draft.

The GAMP Forum Electronic Records and Signatures Special Interest Group would like to thank all those who commented on the first draft, and in particular, the valuable feedback provided by the following:

- Russell E.Masden on behalf of Parenteral Drug Association (PDA)
- Svend Martin Fransen on behalf of Novo Nordisk A/S Health Care
- Robert S. Poulton and Frank Wood on behalf of Smithkline Beecham Pharmaceuticals
- Paul D'Eramo on behalf of Johnson and Johnson Quality & Compliance Services
- Anthony J.Trill (Medicines Control Agency)
- Dr Guy Wingate on behalf of Glaxo Wellcome Manufacturing and Supply

2. OBJECTIVES

In general terms, this document aims to be:

- Representative of current best practice
- Comprehensive in coverage of issues
- Generally applicable within pharmaceutical manufacturing
- Easily readable and referenced
- The basis of continuing discussion

More specifically, and recognising the key role that suppliers have in supporting pharmaceutical manufacturers achieve fully compliant 21 CFR Part 11 applications, the document aims to provide the following information:

- Guidance to pharmaceutical manufacturers on how to implement a 21 CFR Part 11 compliance programme
- Guidance to suppliers on what features are required in their products in order that pharmaceutical manufacturers may implement 21 CFR Part 11 compliant applications
- Clear and practical interpretation of the 21 CFR Part 11 rule
- Information on topics of common interest and concern
- Examples to aid interpretation

3. SCOPE

This document is written for manufacturers of regulated pharmaceutical products and their suppliers and is therefore focused on GMP. Since 21 CFR Part 11 also applies to GCP and GLP regulated areas, much of this GAMP document is therefore directly applicable to the Research and Development function and to the medical device industry. However, no specific consideration has been given to the impact of the regulations in non-GMP situations, such as on the development and use of electronic submissions, or its impact on the manufacture of medical devices.

This document is aimed at manufacturing applications. These are primarily closed systems, using password or other non-biometric security. The issues of open systems and biometric signatures are not therefore covered. There is no intention to promote specific technologies or applications. Examples given are intended to convey how the rule should be applied to common classes of system, rather than to individual products.

Decommissioning of existing systems and the associated transfer and archiving of data are not covered by this document.

The new regulations apply only to products manufactured for sale in the USA. Whilst these standards are likely to be acceptable for most of the rest of the world, the use of electronic

signatures on official documents destined for other countries, e.g. on Certificates of Analysis, may still be problematic and will need to be defined on a case by case basis.

4. MANAGEMENT APPROACH TO ACHIEVING COMPLIANCE

This section provides a management process for pharmaceutical companies to follow to achieve and maintain compliance with 21 CFR Part 11.

The objective of the 21 CFR Part 11 ruling is to:

- Permit the introduction of new technology
- Preserve and protect electronic GxP records
- Prevent fraudulent changes being made to electronic records
- Allow the FDA to operate on the same technological plane as the industry that it regulates

This does not mean that the measures introduced must be infallible. The FDA recognises that both computers and users make mistakes but is seeking to ensure that mistakes are detected and that any obviously fraudulent attempts to manipulate electronic records or to disown the activities carried out under an electronic signature are either prevented or detectable.

For its part, industry recognises that the majority of current applications are not fully compliant with the ruling. Furthermore, future compliance of user applications is dependent on functionality provided by suppliers within their packages. Pharmaceutical companies need to work with their suppliers to promote the provision of technology and packages that inherently support 21 CFR Part 11. At the same time, an immediate objective is to maximise compliance of existing systems within the constraints of the existing system's technology – using operating procedures wherever possible to cover technological limitations.

While many of the controls will already be in place for existing applications used within manufacturing, the additional requirements imposed by 21 CFR Part 11 necessitate a thorough review to ensure continuing compliance.

4.1 INTRODUCTION TO THE APPROACH

This management approach has been developed taking into account the FDA Compliance Policy Guide (CPG) 7153.17 Section 160.850 (see Appendix 6). Key messages in that Guide are:

1. The FDA recognises that it will take time for existing systems to attain full compliance with 21 CFR Part 11.
2. The FDA reaffirms that systems which are still in use, but that predate August 20, 1997 are not exempted from rule. FDA expects firms to be taking steps towards achieving full compliance of these systems with 21 CFR Part 11.
3. When non-compliance situations are found, FDA will include the following points in their evaluation:
   - Nature and extent of 21 CFR Part 11 deviations

- Impact on product quality and data integrity
- Adequacy and timeliness of planned corrective measures (bearing in mind FDA expects that 21 CFR Part 11 requirements for procedural controls should already have been met by pharmaceutical companies)
- Compliance history of the establishment, especially with respect to data integrity

In order to address these messages, the management approach defined in this GAMP document will ensure that:

- Procedural controls required by the new regulation will be implemented quickly.
- There is a plan in place to show how full compliance will be achieved. This involves managing technological changes that will take more time to introduce. However, at any point in time it must be possible to demonstrate progress against the plan.

The approach has three main elements:

1. Initial steps that need to be undertaken
2. Achieving compliance for new systems
3. Achieving compliance for existing systems

These elements are addressed in the remainder of this section.

4.2 ACHIEVING COMPLIANCE - THE FIRST STEPS

There are three initial steps that should be taken towards achieving compliance with 21 CFR Part 11, each of which delivers a tangible objective as shown in Table 1 below.

Table 1. Initial Steps towards Compliance

Step	Activity	Deliverable
1.	Agree the objectives	A set of objectives **agreed** by senior managers
2.	Communicate to everyone	An understanding of the implications of Part 11 for everyone involved Commitment to resolve any non-compliance Inform FDA that electronic signatures are legally binding equivalent of traditional hand-written signatures
3.	Agree an interpretation	An interpretation of what Part 11 means for the individual pharmaceutical company based on this GAMP document

4.2.1 STEP 1 - AGREE THE OBJECTIVES

It is important to be clear about the objectives of the project that will bring systems into compliance. The following is a suggested list:

- To understand the regulation
- To gain management commitment for resources and budgets to solve the problem
- To educate users in their responsibilities under the rule
- To ensure each new system sanctioned is compliant from day one, or to establish controls and action plans to address non-compliances
- To bring existing systems into compliance
- To provide an assessment tool for use with new systems
- To deliver business benefits

Business Benefits of Implementing a Management Approach

The Management Approach described in this section brings both new and existing systems into compliance. While this is the primary aim of the project, it brings with it many other business benefits. These are generally of a "soft" nature, and include:

- Improvement in GMP processes. This arises as a consequence of reinforcing the need to apply GMP in the IT area, an area where many QA people are still uncomfortable.
- Improves corporate understanding of the value of information. Many organisations do not understand the true value of data to their organisations until they have lost it. (A hard drive crash on a PC brings home the value of electronic records within an organisation).
- Review of all systems. The approach outlined here will require that all existing systems are reviewed for cGMP compliance, in much the same way that the Y2k problem ensured that all systems were reviewed for that particular problem.
- More secure and reliable systems. Many of the requirements of 21 CFR Part 11 are aimed at securing the electronic records from accidental loss or corruption. Consequently, this review will improve the reliability and security of existing systems.
- Better understanding by staff of need for integrity of data. The fact that this project is taking place is an opportunity to re-emphasise to staff the importance of data for the commercial as well as regulatory protection.
- Brings "IT" closer to the business. This project can only be completed by working closely with the IT department. It therefore emphasises their role in GMP compliance.

4.2.2 STEP 2 - COMMUNICATE TO EVERYONE

Before starting the detailed work of the project, it is necessary to secure commitment from senior management and to communicate this commitment and the mechanism for achieving the objective to everyone involved.

Senior management should agree the following points:

- The scope of the ruling (that it applies to all systems that contain GMP-relevant electronic records, in addition to systems that utilise electronic signatures).
- How the Part 11 ruling impacts the business (that through the imposition of various controls it enables computerised operations including the use of electronic signatures, which leads to opportunities for efficiencies).
- The impact on new and existing systems (additional validation and the problems of existing systems).
- The FDA's stance (that for existing systems, a period of time is being allowed to bring them into full compliance, although procedural controls should by now be in place. Also that new systems must comply from their conception and introduction. See Appendix 6.).
- The proposed approach following the process described here.
- The resources that will be required for the evaluation and later for the subsequent actions to achieve compliance.

Assuming senior management approval is given, a communication to project teams, system owners, and all users who create or maintain GMP records is necessary. This should focus on:

- The commitment of senior management to comply with the ruling on electronic records and signatures.
- A summary of the issues to be addressed.
- The business benefits.
- The impact on QA and particularly the need to bring existing systems into compliance.
- The impact on users in production, and the controls to which they must adhere, and the impact in the IT department.
- The impact on those delivering new systems into the business (including IT departments and suppliers).
- An outline of the approach agreed.

The step change required in organisational culture due to the introduction of electronic record and signature systems needs to be recognised. The successful implementation and maintenance of electronic systems can only be achieved by people adapting to new ways of working. One of the biggest challenges being that of becoming more dependent on electronic information rather than paper based information.

Staff need to be aware of the security implication and must follow the correct procedures for accessing and leaving electronic systems that employ electronic signatures.

This change in culture can be managed through awareness programs and training.

It is also necessary to inform FDA that electronic signatures are legally binding equivalent of traditional hand-written signatures, in accordance with Subpart C §11.100.

4.2.3 STEP 3 - AGREE AN INTERPRETATION

Within an organisation, it is necessary to agree how the rule will be interpreted. This is best done with a small expert group of people. The interpretation will vary from organisation to organisation, depending on the sophistication of their electronic record systems, but it is essential that an interpretation is agreed and documented. This interpretation can then be communicated across the organisation to ensure a common understanding is known and the expert group can continue to act as arbiters for future questions of interpretation.

The information in this GAMP document will assist individual companies to develop an interpretation of the rule suited to their circumstances. Particularly relevant are:

- Appendix 1 - Annotated 21 CFR Part 11 Rule, The practical interpretation given here is a distillation and assembly of views taken from FDA input to various conferences, published articles, GAMP Forum meetings and GAMP, ISPE and PDA members views.
- Appendix 2 - Types of Controls Required. This gives a list of the company operating procedures that will be required and also the technological controls that are required of Electronic Record and Signature systems. It should be recognised that existing systems in particular will not have all the required technological controls, so the expert group will have to decide how those requirements can be addressed by a combination of practical system and procedural controls.
- Appendix 4 – Key Areas For Guidance. This appendix discusses issues of particular interest, and the subject of current industry focus.
- Appendix 5 – Examples of Applying 21 CFR Part 11

The preamble to the rule published by the FDA provides a great deal of information. At least one member of the expert group should be familiar with its content. Further information may also be found on the FDA web site www.fda.gov.

Most importantly of all, the expert group must apply their knowledge and experience of GMP. Successful compliance is often the application of common sense; this principle is equally applicable when dealing with Electronic Record and Signature systems.

Once prepared and agreed, the interpretation can be used for both new and existing systems.

It is important at this stage that company policies are reviewed and updated as necessary. For example, checks should be made that all applicable local legal regulations are taken into account when implementing electronic signatures. In addition, the rule requires that

companies certify the use of electronic signatures within their organisation as being the legally binding equivalent of traditional hand written signatures. While this can be done at a corporate level, particular attention needs to be paid to ensuring on-going communication of this message to those who need to know, particularly following company re-organisations and corporate activity such as mergers and acquisitions.

4.3 ACHIEVING COMPLIANCE FOR NEW SYSTEMS - GUIDANCE FOR USERS AND SUPPLIERS

Further to the process described in Section 4.2 above, there are five further steps to achieving compliance of new systems, each of which delivers a tangible objective as shown in Table 2 below.

Table 2. The Steps and Deliverables Required to Bring New Systems into Compliance

Step	Activity	Deliverable
1.	Educate project teams	Understanding of how compliance is to be achieved Commitment to resolve any non-compliance
2.	Provide clear requirements to suppliers	List of testable requirements in specifications provided to supplier
3.	Assess the level of compliance of proposed technology	A list of non-compliances
4.	Update Validation Plan to cover compliance with 21 CFR Part 11	Validation Plan showing what activities and procedures are required to provide compliance
5.	Execute the Validation Plan	Documentary evidence of compliance with 21 CFR Part 11

4.3.1 STEP 1 - EDUCATE PROJECT TEAMS

The compliance of current and proposed automated system projects with 21 CFR Part 11 will largely depend upon the project teams responsible for development and delivery of those systems. It is vital that those project teams, and in particular their management, understand the importance of this rule, and their responsibilities for complying with it.

Key messages to communicate include:

- Responsibility for compliance with 21 CFR Part 11 ultimately lies with the pharmaceutical organisation, not the supplier.
- The supplier's role in providing the necessary technological functions and features is critical.
- User operating procedures also form a critical part of achieving compliance.
- Documentary evidence of compliance with the rule is required.
- The activities required to achieve compliance with 21 CFR Part 11 should be identified during contractual negotiations and planned into the project.

The interpretation of Part 11 that was completed as part of Section 4.2.3 above forms the basis for educating the project teams. It should enable pharmaceutical organisations to specify clearly what functions and features are necessary in any new system that is subject

to 21 CFR Part 11 requirements. The interpretation should also indicate what must be validated in those systems before they are accepted for use.

Projects considering electronic document management will find Appendix 7, Electronic Documents and their Management Lifecycle, very useful.

4.3.2 STEP 2 - PROVIDE CLEAR REQUIREMENTS TO SUPPLIERS

Automated systems that have an impact on product quality in the manufacture of pharmaceutical products are subject to GMP. Users and suppliers of such systems are already aware of the need to validate, using guidance such as that provided in the GAMP Guide.

Requirements Specifications for systems that contain either electronic records or signatures need to state clearly what is required from the prospective supplier in order that the user may achieve compliance with 21 CFR Part 11.

Appendix 2 of this GAMP Document lists the technological controls required of any automated system in order that it can be compliant with the rule. The Appendix also clearly identifies supplier responsibilities for meeting the requirements.

When drawing up the Requirements Specification, a clear definition of the business usage should be included, covering:

- What electronic records will exist in the system, and the business processes that create and update them
- Where electronic signatures are to be used both in terms of a business process and the local environmental conditions (i.e. office/gowned up area etc.)
- The purpose of any electronic signatures
- The approval actions to be given by electronic signatures
- What records are being signed (i.e. a data record, a screen of data, a sequence of records etc).

Consideration should also be given to the metadata that support the subject electronic records.

4.3.3 STEP 3 - ASSESS COMPLIANCE OF PROPOSED TECHNOLOGY

Assessing the proposed solution for compliance with 21 CFR Part 11 should occur during pre-contract negotiations, forming an integral part of the supplier and solution selection process. The information needed to complete the assessment and to offer conclusions will come from several sources:

- The supplier audit, already commonly carried out prior to contract placement, can be extended to include 21 CFR Part 11 requirements.

- Prospective suppliers can be requested to respond to the specific 21 CFR Part 11 requirements defined during Step 2 above. This response can then be assessed.
- An internal review of the requirements can be carried out.

Once the assessment is complete, a picture of the degree of compliance of the proposed solution(s) is available. This can be one factor in determining the solution to select, however, there will be times when no solution is 100% compliant. In these situations, there are four alternatives:

1. Delay or cancel the project
2. The supplier is asked to identify how the deficiencies can be surmounted
3. Procedural controls are identified to address the deficiencies
4. The project scope is changed so that the deficiencies are eliminated

Decisions taken at this point will be very important, and will provide vital information for updating the Validation Plan, which is the next step.

4.3.4 STEPS 4 AND 5 - UPDATE AND EXECUTE VALIDATION PLAN

Much of the information necessary to develop the Validation Plan is now available. This will include the sequence of activities and resources necessary to complete the project, in order to provide evidence that the validated system meets the requirements of 21 CFR Part 11. These activities include ensuring that system testing will demonstrate compliance with each relevant clause of the rule. Responsibilities for implementing all Procedural Controls will also be identified, the controls being proven during Qualification.

It should be recognised that there could be cost implications, particularly for bespoke systems, since additional technological controls (i.e. software and/or hardware) will need to be built into the proposed system and tested. However, it is better to identify these extra activities and plan for them, rather than be faced with late changes to the scope as the impact of the rule becomes evident in later stages of the project.

It will be important to keep the Validation Plan under review. In the short term evolving interpretations of the Part 11 rule may mean that revisions to the plan will be necessary.

Further information on producing Validation Plans is provided in the GAMP Guide.

4.4 ACHIEVING COMPLIANCE FOR EXISTING SYSTEMS

Further to the process described in Section 4.2 above, there are five further steps to achieving compliance of existing systems, each of which delivers a tangible objective as shown in Table 3 below.

Table 3. The Steps and Deliverables Required to Bring Existing Systems into Compliance

Step	Activity	Deliverable
1.	Form the team	Resources to perform the evaluation task
2.	Assess the level of compliance for each system	A list of compliant systems A list of non-compliant systems and their non-compliance
3.	Evaluate the extent of non-compliance and agree actions	A prioritised list of systems to bring into compliance
4.	Write a master plan to achieve compliance for all existing systems	A plan against which to measure progress towards compliance
5.	Execute the plan	Systems back in compliance according to the plan

4.4.1 STEP 1 - FORM THE TEAM

Before forming the team, it is necessary to identify a Project Sponsor - someone who will champion the cause at the highest level in the company. This is necessary because the detailed evaluation of existing systems and resulting corrective action, as will be seen later, may require considerable resources.

The team involved with the initial evaluation of systems compliance with Part 11 could be quite small. It may require only three or four people per site as follows:

- A Team Leader to develop the evaluation process and manage it through.
- An Assessor to carry out the assessment (this could be the same person as the Team leader unless the organisation is very large).
- A representative from IT preferably with a Quality Management background to clarify any technical issues.
- The System Owner as needed (on a system by system basis).

At least one of these individuals needs to be familiar with cGMP in relation to 21 CFR Part 11.

This team will carry out Steps 2 through 4 in Table 3 above, and can be involved in supporting Step 5.

4.4.2 STEP 2 - ASSESS THE LEVEL OF COMPLIANCE FOR EACH SYSTEM

Having agreed upon the interpretation of the rule, the next step is to assess the current level of compliance of existing systems. This is best carried out as a two-part process:

- Part 1 – For each system, assess whether 21 CFR Part 11 applies.
- Part 2 – For those systems where it does apply, how extensive is the non-compliance?

Part 1.

Start with a list of systems (the year 2000 list is a good place to start in the absence of any other). It should be noted that it is a requirement of GMP that such a list is maintained. From the list, evaluate each system to see whether 21 CFR Part 11 applies. This is most easily done with a simple checklist as follows:

- Is the system involved in a GMP process?
- If so, does it capture GMP data?
- If so, does it retain GMP data on durable media? 21 CFR Part 11 on electronic records applies if the answer to this question is "Yes".
- Do staff confirm electronically that they are performing a GMP task, and does this action replace a hand written signature as required by the regulation? 21 CFR Part 11 on electronic signatures applies if the answer to this question is "Yes".

Key to answering the above questions is an understanding of what electronic records and signatures exist within the system. Consideration should also be given to all metadata that support these records.

The output from this evaluation therefore is a list of systems to which 21 CFR Part 11 applies and which require evaluation that is more detailed. Part 11 does not apply to any other systems. The records of this process provide a rationale for the inclusion and exclusion of systems from the project and should be signed by the system owner, the assessor and QA.

Part 2.

Detailed evaluation is again most easily carried out with a checklist.

A suitable checklist is attached as Appendix 3. This checklist is derived directly from the ruling and divided into five sections as follows:

- Procedures and controls for closed systems
- Procedures and controls for open systems
- Electronic signatures (3 sections; general, biometric and non-biometric)
- Controls for identification and password entry

- Controls for token cards and devices delivering identification codes

The checklist may be presented as a table with separate columns to record comments, and the recommended corrective action for each non-compliance. Some companies may develop a scoring system to give a more quantitative feel. Recording non-compliances in this way will allow judgements to be made on the extent of non-compliance of the whole company or site, which will be useful in the next stage.

4.4.3 STEP 3 - EVALUATE THE NON-COMPLIANCE

The final stages of the evaluation include:

- Evaluating the results of the assessment
- Evaluating the priority
- Deciding on the action to be taken, system by system
- Documenting the decisions

There are only five options available for each system:

1. Stop the activity. This option should be considered but will not contribute significantly to reducing the workload. It is possible that some old and/or small systems, typically small developments in the laboratory, may not contribute significantly to GMP and so it is not worthwhile upgrading them and the activity can be stopped.
2. Retire the system and return to paper. This too may apply to the same sort of system. The cost of upgrading may not be worth the value contributed by the system. However, if it contains some electronic records they must also be "retired", Continued access to the "retired" records can be achieved, by retaining the hardware and software and restricting access to a few senior authorised individuals for reviewing complaints or recalls.
3. Implement procedural controls. This may be the most commonly used option. Procedures, and training in their use, will be implemented to address gaps in compliance with the rule.
4. Replace the system. This may be the most cost-effective and quickest option, but the cost and workload will preclude doing this for every system.
5. Upgrade the system. This may be a large or small task and input from IT professionals is necessary to make a meaningful evaluation. The implication may be significant and other options might be considered more cost-effective.

In making the evaluation, the scoring system used in the evaluation will help in both the assessment and the prioritisation. Factors affecting the prioritisation include:

- The GMP criticality of the system
- The extent of non-compliance (large, medium or small)

- The security and integrity of the data (or lack of it)
- The age of the system and when it is expected to be "retired"

The completion of this process will result in:

- The list of systems to be brought into compliance
- The non-compliance to be resolved
- The action to be taken for each system
- The order in which they will be brought into compliance

These are the major inputs to the final steps.

4.4.4 STEPS 4 AND 5 - DEVELOP AND EXECUTE A MASTER PLAN

Much of the information necessary to develop the Master Plan is now available. This needs to be developed in the same way one develops a Validation Master Plan with the sequence of events and resources necessary to complete the project. This allows costs to be estimated but a decision is still necessary from senior management before the project is started.

The cost is likely to be high for a major company and budgeting restraints may mean some revision to the plan before it is finally approved.

It will be important to review the master plan from time to time. Company system strategies and evolving interpretations of the Part 11 rule may mean that significant revisions to the plan will be necessary.

5. CONCLUSIONS

21 CFR Part 11 is one of the most significant piece of new rule-making for over a decade. It revolutionises industry's ability to implement new and more efficient technology in the regulated pharmaceutical manufacturing environment. This opportunity to remain competitive by exploiting the new tools now available must not be missed.

That means the rule must be interpreted and applied, first to new systems "still on the drawing board" and secondly to existing systems so that they may be brought back into compliance. This needs to be done in the most cost-effective and expedient way without impeding any new development.

This document provides clear interpretation of the rule, provides a management approach for pharmaceutical organisations to achieve and maintain compliance, and highlights those areas that require action by suppliers.

Pragmatism is what is demanded – not heroic efforts. Using the information provided in this document, pharmaceutical organisations can conduct a review of systems to identify those directly impacted by 21 CFR Part 11. This should be followed by a detailed evaluation of each impacted system. The results will enable the scale and depth of non-compliance to be identified and Master Action Plans formulated to meet the regulations. This in turn will enable industry to proceed decisively and confidently with the application of technological advances in this specific area.

6. APPENDICES

1. Annotated 21 CFR Part 11 Rule
2. Types of Controls Required
3. System Assessment Checklist
4. Key Areas for Guidance
5. Examples of Applying 21 CFR Part 11
6. FDA Compliance Policy Guide; Enforcement Policy: 21 CFR Part 11
7. Electronic Documents and their Management Lifecycle
8. Examples from Warning Letters
9. Glossary
10. References

6.1 APPENDIX 1 - ANNOTATED 21 CFR PART 11 RULE

The practical interpretation given here is a distillation and assembly of views taken from:

- FDA input to various conferences
- Published articles
- GAMP Forum meetings
- GAMP, ISPE and PDA members views

Where appropriate, FDA comments from the Federal Register have been included verbatim in the annotations column. These are italicised, and enclosed in Quotation marks, e.g. "*Example text*".

For brevity, the following abbreviations are use in the Annotations column:
ER: Electronic record
ES: Electronic signature
CS: Computer System(s)

Text of 21 CFR Part 11	Annotation
PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES	
Subpart A—General Provisions Sec. 11.1 Scope. 11.2 Implementation. 11.3 Definitions.	Rule states FDA view is that the risks of falsification, misinterpretation, and change without leaving evidence are higher with electronic records than paper records, and that therefore specific controls are required.
Subpart B—Electronic Records 11.10 Controls for closed systems. 11.30 Controls for open systems. 11.50 Signature manifestations. 11.70 Signature/record linking.	*"...people determined to falsify records may find a means to do so despite whatever technology or preventive measures are in place. The controls in part 11 are intended to deter such actions, make it difficult to execute falsification by mishap or casual misdeed, and to help detect such alterations when they occur "*
Subpart C—Electronic Signatures 11.100 General requirements. 11.200 Electronic signature components and controls. 11.300 Controls for identification codes/ passwords. Authority: Secs. 201–903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321–393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).	Note that the *"ultimate responsibility for Part 11 will generally rest with persons responsible for electronic record content, just as responsibility for compliance with paper record requirements generally lies with those responsible for the record's content"*

Text of 21 CFR Part 11	Annotation
Subpart A—General Provisions	
§ 11.1 Scope.	
(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.	For ERs created before the effective date, those regulations relating to creation do not apply - such records do not therefore need to be adjusted retrospectively to comply. Regulations relating to modification, such as audit trails for record changes and the requirement that original entries must not be lost when new versions are added, apply only to modifications to ERs on or after the effective date. Maintenance provisions, such as measures to ensure that electronic records can be retrieved throughout their retention periods, apply only to ERs modified on or after the effective date. Lack of comment on existing systems by FDA during inspections before the effective date does not imply acceptance or endorsement. Existing ERs and ESs will be assessed on a case by case basis
(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and	Does not apply to CS incidental to creation of records stored and maintained on paper (e.g. word processor).

Text of 21 CFR Part 11	Annotation
the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.	Does not apply to paper faxes.
(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.	This provision addresses the relationship of part 11 to other regulations and the equivalence of electronic records and electronic signatures
(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.	
(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.	*"...it may be necessary to inspect hardware and software used to generate and maintain electronic records to determine if the provisions of part 11 are being met. Inspection of resulting records alone would be insufficient.*" Maintenance of obsolete CS solely to enable FDA inspection is not required. Documentation relevant to Part 11, however, must be available for inspection while the ERs are required by regulations.

Text of 21 CFR Part 11	Annotation
	While the ERs are required, either original CS capable of reading them must be maintained or a complete and accurate, validated, transcription to another system performed.
§ 11.2 Implementation.	
(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.	The regulations do not require, but do permit, the use of electronic records and signatures. Traditional paper documents and signatures can continue to be used. It is also possible to use paper records for some systems and electronic for others. It is not all or nothing. See Section 6.4.4 Hybrid Systems.
(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that: (1) The requirements of this part are met; and (2) The document or parts of a document to be submitted have been identified in public docket No. 92S– 0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of	This provision provides the conditions under which electronic records or signatures can be submitted to the FDA by pharmaceutical companies in lieu of paper.

Text of 21 CFR Part 11	Annotation
documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.	
§ 11.3 Definitions.	
(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part. (b) The following definitions of terms also apply to this part: (1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)). (2) Agency means the Food and Drug	There is no list of ‘acceptable’ biometric methods.

Text of 21 CFR Part 11	Annotation
Administration. (3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.	The use of biometric identification is not mandatory but should be considered carefully as an option for Open Systems (see provision § 11.30 below**)**. It is viewed as being less prone to being compromised than other methods. An electronic signature comprising two distinct identification components, such as an id-code and password, is equally acceptable to FDA but the demands for system controls are more stringent.
(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.	Where access over public phone lines is permitted, but controlled by the persons responsible for the electronic records the system can be considered closed. However, additional controls ought to be considered in such cases, such as input device checks, call backs, security cards. (Contrast with Open System below)
(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. (6) Electronic record means any combination of	

Text of 21 CFR Part 11	Annotation
text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.	
(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.	Handwritten signatures can be captured and recorded electronically. These are not classified as electronic signatures and are not therefore subject to the controls associated with electronic signatures. They are however still subject to the controls associated with electronic records.
(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate 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.	
(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	The ability to access a system via a modem does not necessarily make it an open system. It depends upon who is responsible for controlling access. Contrast with 'Closed System' above.
Subpart B—Electronic Records	
§ 11.10 Controls for closed systems.	
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed	These controls apply from the time electronic records are created, not from official acceptance of the record, depending on the predicate rule.

Text of 21 CFR Part 11	Annotation
to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	FDA encourages firms to include in their internal audit programmes periodic audits for compliance of computer systems with the rule. *"Self audits…may be considered as a general control, within the introductory paragraph of § 11.10"*
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The agency will expect evidence that all validation activities, as carried out today for other computer systems, have been completed for each ER/ES system. This includes, but is not limited to, planning, specification, testing, QA review and approval. Discerning invalid/altered records involves the ability to identify when changes were made, by whom, and whether these were authorised.
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	Firms need not maintain obsolete equipment in order to make copies that are 'true' with respect to format and computer system. However, when moving to new technology, a complete transcription of the data, including all supporting 'metadata' must be made and formally verified.
Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	FDA may want to use computerized methods to audit electronic records to detect trends, inconsistencies and problem areas. The audit could occur on-site, or copies of the records could be taken off-site for subsequent

Text of 21 CFR Part 11	Annotation
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	review. Pharmaceutical companies should specify their retention periods and ensure the security of the records (e.g. by maintaining backups).
(d) Limiting system access to authorized individuals.	This can include limits within a system to levels of access and is described in EU Annex 11 and GAMP Appendix 4
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	The audit trail should capture actions at the date and time they occur, and must be created by the system independently of operators. Reliable time stamping of events is critical, and this process should be proven to be accurate and secure from unauthorised alteration, and the time stamp should be unambiguous.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	These checks only apply where a process must be followed in a pre-defined order.
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	This involves a combination of physical access measures, which may include procedures, system defined logical access controls, and/or pre-defined electronic signatories for each type of record.

Text of 21 CFR Part 11	Annotation
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	These checks only apply where certain devices have been specified as legitimate sources of data or commands. The need for such checks should be identified during system specification.
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	The check of personnel qualifications need not be performed automatically by the computer system. Some on-the-job training would be expected, and should be documented. Supplier staff must also be qualified. Formal examination and/or certification, while desirable, is not a requirement.
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Employees need to understand the gravity and consequences of signature or record falsification. Where one individual signs on behalf of someone else, e.g. as a deputy, the signature applied must be that of the person signing, with some record of that fact.
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Systems documentation includes help files, operations manuals, SOPs, security and access information, operating systems manuals. This provision pertains to systems documentation that can be changed by individuals within the pharmaceutical company, and applies to systems once released for use. If documentation can only be changed by the supplier, this provision does not apply to the supplier's customers. Electronic systems documentation requires an automatic

Text of 21 CFR Part 11	Annotation
	electronic audit trail. Paper systems documentation can have a paper or electronic audit trail.
§ 11.30 Controls for open systems. Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	Additional controls are specified in recognition of the extra risks associated with open systems.
§ 11.50 Signature manifestations. (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	The information can be stored within the electronic record or in logically associated records, but must always be shown whenever the record is displayed/printed.
(1) The printed name of the signer;	This may not be, in itself, unique. An identification code is not an acceptable substitute for the name of the signer.
(2) The date and time when the signature was executed; and (3) The meaning (such as review, approval,	

Text of 21 CFR Part 11	Annotation
responsibility, or authorship) associated with the signature. (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	
§ 11.70 Signature/record linking. Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Any appropriate method can be used to link electronic signatures to their respective electronic records to prevent falsification. Digital signatures is one method, as is use of software checks to prevent the electronic signature from being copied or removed. It must not be possible to remove a signature and re-apply it elsewhere on a record by the use of standard functions.
Subpart C—Electronic Signatures **§ 11.100 General requirements.** (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Individuals may sign electronically on behalf of others, but must use their own electronic signature to do so. The records must show who actually signed and in what capacity (e.g. on behalf of ... in this case the duty is delegated, but not signature manifestation) Where an id-code/password is used as an electronic signature specific controls apply (see Section 11.300) Common group id-code/passwords may be established for read only purposes but must not be used as electronic

Text of 21 CFR Part 11	Annotation
	signatures.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	The physical identity of the person should be confirmed, as should the validity of granting the authority associated with a particular electronic signature to a known person, e.g. by a line management approval, authorised by the system owner.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	This certification can be confirmed at an organisational level. It need not occur for each system but must be done before the use of ES in any system. A suggested format is provided in the preamble to the Rule on page 13456 in paragraph 120.
§ 11.200 Electronic signature components and controls. (a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification	System administrators should not know another person's

Text of 21 CFR Part 11	Annotation
components such as an identification code and password.	password. They would be expected to have privileges allowing them to assist individuals who forget passwords
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	Continuous period of controlled system access means the user being at the computer terminal, or having put the terminal into a secure 'pause' state. It could be useful to review processes to ensure signatures are used only where required and not for convenience
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	When several single component signatures are applied during the same session, the screen must display the user name throughout the session.
(2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	This includes the electronic signature's owner disclosing the password to a second person. Using another person's signature (even on behalf of them) would be record falsification. The implemented design to prevent falsification should be verified as part of system validation.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Where combinations of biometric/non-biometric signatures are used, the regulatory requirements for each element of the combination will apply.
§ 11.300 Controls for identification codes/	

Text of 21 CFR Part 11	Annotation
passwords. Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	This section does not apply where: (1) persons use electronic signatures not based on id-code/password, (2) persons use handwritten signatures, (3) the electronic record is not signed at all. The id-code need not be private, and may be electronically displayed on screen. As password uniqueness cannot be guaranteed, then id-codes must be unique. Rules and guidelines on defining passwords (e.g. minimum lengths, avoiding common words) are recommended. The key point is that the use of an id-code/password combination is directly attributable to one individual. Therefore, each combination must be unambiguous within the context of its use.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	This provision would be met by ensuring that people change their passwords periodically, obsolete users are removed promptly, and the profiles of users whose roles have changed are updated promptly.
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Preventative measures such as training on safekeeping of such devices should be implemented. After a password is lost or compromised, it should be reset as quickly as possible.

Text of 21 CFR Part 11	Annotation
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Systems should signal attempted, unsuccessful, access, in order that procedural action can be undertaken. Companies should define what constitutes an attempt at unauthorized use. Typically, the user-id should be locked out after a specified number of failed attempts. The implementation of other safeguards should also be considered, e.g. system knowledge of a person's unavailability (e.g. leave of absence)
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	This provision applies to devices used as components of an electronic signature. Proper device functioning includes permitting system access, correctness of identifying information, and security performance attributes (e.g. expiration date). Renewal on a regular basis would be an alternative. Testing should also check for cover wear and tear, which could be carried out during internal audits.

Dated: March 11, 1997. William B. Schultz, Deputy Commissioner for Policy. [FR Doc. 97–6833 Filed 3–20–97; 8:45 am]
BILLING CODE 4160–01–F

6.2 APPENDIX 2 - TYPES OF CONTROLS REQUIRED

This table defines procedural and technological controls required to fully support 21 CFR Part 11. It is recognised that not all these technological controls are currently available in commercial s/w packages. Software vendors should be aware of these requirements when contemplating package developments.

Primary responsibilities for the controls are assigned as follows:

P – Pharmaceutical manufacturing organisation which is going to use ER/ES system in regulated environment
S - Supplier of ER/ES System (this could of course be a separate internal function of the pharmaceutical organisation, such as the Information Systems department)

It is also noted that this table can be utilised by pharmaceutical organisations when carrying out audits of prospective suppliers of automated systems that are subject to 21 CFR Part 11. The existence of those controls identified as being the prime responsibility of the supplier should be checked during the audit, and action taken to address any deficiencies.

Clause	Type of Control	Resp	Notes
11.10	Procedural	P	This clause specifies a number of specific controls. The pharmaceutical organisation will need to demonstrate a system of self-inspection audits to demonstrate compliance with the procedures and controls listed below.
11.10 (a)	Procedural	P	ER/ES systems need to be validated. An industry-recognised approach is given in GAMP. This validation should include documented verification that the system provides the required controls for 21 CFR Part 11 compliance – for example, the ability to discern invalid records, ability to generate copies of records, provision of adequate audit trail, etc.
	Technological	S	ER/ES system should be able to identify changes to electronic records in order to detect invalid or altered records. In practice, this means having an adequate audit trail that can be searched for information. For example, to determine whether any changes have been made without the appropriate authorisations.
11.10 (b)	Technological	S	ER/ES systems should allow electronic data to be accessed in human readable form.
11.10 (b)	Technological	S	ER/ES systems need ability to export data and any supporting regulatory information (e.g. audit trails, configuration information relating to identification and status of user s and equipment)

Clause	Type of Control	Resp	Notes
11.10 (c)	Procedural	P	Pharmaceutical organisations should specify retention periods (in accordance with predicate rules) and responsibilities for ensuring data is retained securely for those periods.
	Procedural	P	Pharmaceutical organisation needs a defined, proven, and secure backup and recovery process for electronic data.
	Technological	S	ER/ES Systems should be able to maintain electronic data over periods of many years regardless of upgrades to the software and operating environment.
11.10 (d)	Procedural	P	Pharmaceutical organisation needs procedures defining how access is limited to authorised individuals. See GAMP Appendix 4, Section 3. Managing super-user account should be given special consideration.
	Technological	S	ER/ES Systems should restrict access in accordance with pre-configured rules that can be maintained. Any changes to the rules should be recorded.
11.10 (e)	Procedural	P	Pharmaceutical organisation needs procedure to maintain the audit trail (see 11.10 (c) above)
	Technological	S	ER/ES systems should be capable of recording all electronic record create, update, and delete operations. Data to be recorded must include as a minimum: time and date, unambiguous description of event, and identity of operator. This record should be secure from subsequent unauthorised alteration.
11.10 (f)	Technological	P S	Where operations are required in a pre-defined order, for example in batch manufacture, the ER/ES system should enforce that ordering through the system's design.
11.10 (g)	Procedural	P	Pharmaceutical organisation needs procedures defining how the authorisation processes are carried out and that staff have been trained in their use.
	Technological	S	ER/ES Systems should restrict use of system functions and features in accordance with pre-configured rules that can be maintained. Any changes to the rules should be recorded.
11.10 (h)	Technological	P S	Where pharmaceutical organisation requires that certain devices act as sources of data or commands, the ER/ES system should enforce the requirement.
11.10 (i)	Procedural	P	Pharmaceutical organisation's staff who develop, maintain or use electronic record/electronic signature systems must have the education, training, and experience to perform their assigned tasks.
		S	Supplier requires procedure to demonstrate that persons who develop and maintain electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Clause	Type of Control	Resp	Notes
11.10 (j)	Procedural	P	Policy needed to describe the significance of electronic signatures, in terms of individual responsibility, and the consequences of falsification both for the pharmaceutical organisation and for the individual.
11.10 (k)	Procedural	P	Pharmaceutical organisation needs procedures covering distribution of, access to, and use of operational and maintenance documentation once the system is in operational use.
	Procedural	P	Pharmaceutical organisation must ensure adequate change control procedures for operational and maintenance documentation.
	Technological	S	Where systems documentation is in electronic form, an electronic audit trail should be maintained, in accordance with 11.10 (e) above.
11.30			Open Systems – not covered by this document.
11.50	Technological	S	ER/ES Systems must ensure signed electronic records contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. These items are subject to the same controls as other electronic records The information can be stored within the electronic record or in logically associated records, but must always be shown whenever the record is displayed/printed.
11.70	Technological	S	ER/ES systems must provide a method for linking electronic signatures, where used, to their respective electronic records, in a way that prevents the signature from being removed, copied or changed to falsify that or any other record
11.100 (a)	Procedural	P	Pharmaceutical organisation must ensure uniqueness of electronic signature, and that they are not re-used or re-allocated.
	Technological	S	ER/ES System should enforce uniqueness, prevent re-allocation of electronic signature, and prevent deletion of information relating to the electronic signature once it has been used.
11.100 (b)	Procedural	P	Pharmaceutical organisation needs to verify the identity of individuals being granted access to ER/ES system.
11.100 (c)	N/a		See annotated rule (Section 6.1 above).

Clause	Type of Control	Resp	Notes
11.200 (a)(1)	Technological	S	ER/ES systems providing non-biometric electronic signatures need at least two distinct components.
11.200 (a)(1)	Procedural	P	Pharmaceutical organisation needs to establish how it will ensure that both components of electronic signature are entered if session has not been continuous (this can be through system design, or operating procedure if necessary).
	Technological	S	ER/ES system should enforce that both components are entered at least at the first signing, and following a break in the session.
11.200 (a)(2)	Procedural	P	Pharmaceutical organisation must ensure staff only use their own electronic signature, not anyone else's even on their behalf, as that would be falsification (see also 11.10 (j))
11.200 (a)(3)	Procedural	P	Pharmaceutical organisation needs procedure that users do not divulge their electronic signature (e.g. passwords)
	Technological	S	ER/ES System should not provide any ordinary means of accessing electronic signature information.
11.200 (b)			Biometrics – not included in this document.
11.300 (a)			Already covered in 11.10 (a) above.
11.300 (b)	Procedural	P	Pharmaceutical organisation needs procedures to cover: removal of obsolete users; changing of profiles as user roles change; periodic checking of identification codes and passwords for inconsistencies with current users; periodic changing of passwords.
	Technological	S	System should force passwords to be periodically changed and also enable id/password combinations to be rendered inactive without losing the record of their historical use.
11.300 (c)	Procedural	P	Pharmaceutical organisation needs procedure for management of lost passwords.
11.300 (d)	Procedural	P	Pharmaceutical organisation needs procedure to describe how response to attempted or actual unauthorised access is managed.
	Technological	S	System should provide notification of attempted unauthorised access and should take preventative measures (e.g. lock a terminal after a specified number of failed attempts, retain card).
11.300 (e)	Procedural	P	Pharmaceutical organisation should define how any devices or tokens that carry user/id or password information are periodically tested and renewed.

6.3 APPENDIX 3– SYSTEM ASSESSMENT CHECKLIST

System Assessment Report
Relating to Electronic Records; Electronic Signatures;
Final Rule, 21 CFR Part 11

System: _____

To be Completed by Reviewer	
Reviewers	
Date(s) of Review	
Persons Contacted during review	
Documentation Referenced in Review	

Completed by: _____ Name: _____ Title: _____ Date: _____

Assessment Approved by: _____ Name: _____ Title: _____ Date: _____

Assessment Approved for

Compliance with CFR by: _____ Name: _____ Title: _____ Date: _____

1. Procedures and Controls for Closed Systems

	Question	Yes	No	Comments	Recommended Corrective Action
11.10(a)	Is the system validated ?				
11.10(a)	Is it possible to discern invalid or altered records ?				
11.10(b)	Is the system capable of producing accurate and complete copies of electronic records on paper?				
11.10(b)	Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA?				
11.10(c)	Are the records readily retrievable throughout their retention period ?				
11.10(d)	Is system access limited to authorised individuals ?				
11.10(e)	Is there a secure, computer generated, time stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?				
11.10(e)	Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change) ?				
11.10(e)	Is an electronic record's audit trail retrievable throughout the record's retention period ?				
11.10(e)	Is the audit trail available for review and copying by the FDA ?				
11.10(f)	If the sequence of system steps or events is important, is this enforced by the system (e.g. as would be the case in a process				

	Question	Yes	No	Comments	Recommended Corrective Action
	control system) ?				
11.10(g)	Does the system ensure that only authorised individuals can use the system, electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations ?				
11.10(h)	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).				
11.10(i)	Is there documented training, including on the job training for system users, developers, IT support staff ?				
11.10(j)	Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures ?				
11.10(k)	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled ?				
11.10(k)	Is there a formal change control procedure for system documentation that maintains a time sequenced audit trail of changes ?				

2. Additional Procedures and Controls for Open Systems

	Question	Yes	No	Comments	Recommended Corrective

					Action
11.30	Is data encrypted ?				
11.30	Are digital signatures used ?				

3. Signed Electronic Records

	Question	Yes	No	Comments	Recommended Corrective Action
11.50	Do signed electronic records contain the following related information? - The printed name of the signer - The date and time of signing - The meaning of the signing (such as approval, review, responsibility)				
11.50	Is the above information shown on displayed and printed copies of the electronic record ?				
11.70	Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification ?				

4. Electronic Signatures (General)

	Question	Yes	No	Comments	Recommended Corrective Action
11.100(a)	Are electronic signatures unique to an individual ?				
11.100(a)	Are electronic signatures ever reused by, or reassigned to, anyone else?				
11.100(b)	Is the identity of an individual verified before an electronic signature is allocated ?				

5. Electronic Signatures (Non-biometric)

	Question	Yes	No	Comments	Recommended Corrective Action
11.200(a)(1)(i)	Is the signature made up of at least two components, such as an identification code and password, or an id card and password ?				
11.200(a)(1)(ii)	When several signings are made during a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session)				
11.200(a)(1)(iii)	If signings are not done in a continuous session, are both components of the electronic signature executed with each signing ?				
11.200(a	Are non-biometric signatures only used by their genuine				

) (2)	owners ?				
11.200(a) (3)	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals ?				

6. Electronic Signatures (Biometric)

	Question	Yes	No	Comments	Recommended Corrective Action
11.200(b)	Has it been shown that biometric electronic signatures can only be used by their genuine owner ?				

7. Controls for Identification Codes and Passwords

	Question	Yes	No	Comments	Recommended Corrective Action
11.300(a)	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password ?				
11.300(b)	Are procedures in place to ensure that the validity of identification codes are periodically checked?				
11.300(b)	Do passwords periodically expire and need to be revised ?				
11.300(b)	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred ?				
11.300(c)	Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost ?				
11.300(d)	Is there a procedure for detecting attempts at unauthorised use and for informing security ?				

11.300(d)	Is there a procedure for reporting repeated or serious attempts at unauthorised use to management ?				

For tokens, cards, and other devices bearing or generating identification code or password information:

	Question	Yes	No	Comments	Recommended Corrective Action
11.300(c)	Is there a lost management procedure to be followed if a device is lost or stolen ?				
11.300(c)	Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised ?				
11.300(c)	Are there controls over the issuance of temporary and permanent replacements ?				
11.300(e)	Is there initial and periodic testing of tokens and cards ?				
11.300(e)	Does this testing check that there have been no unauthorised alterations?				

6.4 APPENDIX 4 - KEY AREAS FOR GUIDANCE

This Appendix provides more detailed advice in the following areas:

- Where to apply Electronic Signatures
- Audit trails
- Signature and record linking
- Hybrid systems
- Continuous periods of use
- Device checks
- Operational checks
- Use of current e-mail technology

6.4.1 WHERE TO APPLY ELECTRONIC SIGNATURES

In general, 21 CFR Part 11 describes the requirements, which must be met when using electronic records and electronic signatures, but does not describe where they are required.

It is the responsibility of the pharmaceutical company to define where electronic records are used and which signatures will be applied as electronic signatures. Whenever an electronic signature is applied, it should be clear when, why and by whom.

It should also be noted that electronic signatures are themselves information items in electronic records.

Where technology does not currently permit the use of electronic signatures, the system must be treated as a hybrid system. This topic is covered further in section 6.4.4.

Electronic signatures are only those that replace hand written signatures as required by the regulation, e.g. as stated in the GMP regulations below.

§ 211.182 Equipment Cleaning and Use Log
The persons performing and double-checking the cleaning and maintenance shall date and sign or initial the log indicating that the work was performed.

§ 211.186 Master Production and Control Records
(a) To assure uniformity from batch to batch, master production and control records for each drug product, including each batch size thereof, shall be prepared, dated, and signed (full signature, hand written) by one person and independently checked, dated and signed by a second person.

§ 211.186 Master Production and Control Records
(8) A description of the drug product containers, closures, and packaging materials including a specimen or copy of each label and all other labeling signed and dated by the persons responsible for approval of such labeling;

§ 211.188 Batch Production and Control Records
(a) An accurate reproduction of the appropriate master production or control record, checked for accuracy, dated, and signed;

§ 211.194 Laboratory Records
(a)(7) The initials or signature of the person who performs each test and the date(s) the tests were performed.

(a)(8) The initials or signature of a second person showing that the original records have been reviewed for accuracy, completeness, and compliance with established standards.

§ 211.192 Production Record Review
All drug product production and control records, including those for packaging and labeling, shall be reviewed and approved by the quality control unit to determine compliance with all established, approved written procedures before a batch is released or distributed.

Electronic signatures may also be used where required by internal procedures to support GMP data. Examples of these could be:

- Approvals for data capture or electronic logs.
- Approvals for documents and procedures
- Approvals for support processes such as change control
- Approvals for non-compliance and deviation reports
- Approvals for new or changed user access authorization
- Approvals for approved suppliers

To avoid any confusion, it is recommended that a complete list be made of processes and the process steps where electronic signatures are used. This list can be used at the outset for planning and checking the degree of compliance with 21 CFR Part 11.

Process steps implemented by software that includes password technology, but which are not an electronic signature as defined above, do not have to be audited against these regulations.

6.4.2 AUDIT TRAILS

This section considers 21 CFR Part 11.10(e) and applies equally to hybrid systems and fully electronic systems. Note that European GMP Guide Annex 11, Clause 10 also covers Audit Trails.

Where an electronic system has audit trail functionality then this keeps track of any entries and changes in the electronic record. At the time of writing, many systems do not have this functionality. In such cases, a manual audit trail must be a maintained in a separate and parallel paper record.

Audit trails are required for operator actions or entries that create, modify, or delete electronic records. Examples of such actions are entry of process data, updates to the batch record, electronic signatures, or material status changes.

Audit trails are also one method of recording completion of important system functions such as password changes, backups.

The audit trail shall contain information about who, what and when. The date and time of the record shall be recorded together with the identity of the person making the record.

The need for an audit trail entry does NOT imply the need for a signature (electronic or manual).

Information relating to changes to records shall not overwrite the audit trail of the original record so it should be possible to establish the current value and all previous values of an electronic record by using the audit trail. It must not be alterable by any operator by any normal means.

The audit trail may be part of, or separate from, the electronic record but must be created by the computer system independently of the operator. Retention requirements for the audit trail are the same as for the subject records.

Verifying the audit trail functionality should be included in the system validation.

The audit trail and the record to which it applies may be linked by the description in the audit trail of the record being updated, and/or the time-stamp.

EXAMPLE AUDIT TRAIL (Note: does not imply any preferred format)

FILE REF	NAME	TIME	DATE	Record Name	DATA VALUE	Unit	Action
Bx5 ProdX	Jim Smith	12:45:17	13 July 1999	Temperature1	55	Deg C	Modify
Bx23 Prod	Rita	12:40:0	13 July	Pressure1	17	Bar	Create

Z	Davies	3	1999				
Bx23 Prod	Rita	09:32:4	13 July	Weight3	2362	g	Create
Z	Davies	5	1999				
Bx23 Prod	Fred	11:15:2	12 July	Weight3	Deleted	g	Delete
Z	Jones	1	1999				
Bx23 Prod	Fred	11:10:0	12 July	Weight3	2632	g	Modify
Z	Jones	6	1999				
Bx23 Prod	Fred	11:01:4	12 July	Weight3	2630	g	Create
Z	Jones	3	1999				
Bx23 Prod	Jim	10:13:4	12 July	Weight2	1750	g	Create
Z	Smith	2	1999				

6.4.3 SIGNATURE AND RECORD LINKING

The regulation requires that electronic signatures be stored in such a way that they can be linked to their respective electronic records to ensure no removal, copying or changing of the electronic signature. Four possibilities exist:

1. The signature is stored within the subject electronic record
   No explicit linking required as it forms part of a single file.

2. The signature is stored separately from record
   The signature should be created with an attribute or combination of attributes that is unique to the subject record. For example, the create/modify time & date if at sufficient resolution, together with the key parameters of the record (including record name, version).

3. Hand-written signature on paper printout from system
   As for 2 the printout should be clearly linked to the record by unique attributes

4. Signature on unrelated paper
   The signatory manually records the unique attributes described in 2 and signs and dates the document

6.4.4 HYBRID SYSTEMS

The regulation puts forward requirements for full electronic systems; where approvals are electronic, the masters are electronic and the records have to be maintained in electronic form. At the other extreme, are the traditional paper-based systems, with paper masters, the approvals written and the paper record maintained.

These two are at opposite ends of the spectrum but most current systems are in between and this is likely to remain for some time until suppliers build the necessary technology into their products to support 21 CFR Part 11

requirements. These are known as hybrid systems, and there is nothing in the ruling to say that such hybrid systems are unacceptable.

An example is a system where the original data is electronic and the system outputs a paper record, which is then signed. The paper does not prevent the original record within the system from being an electronic record. There is a need to ensure that the paper print out is a complete and accurate record of the master and there is a need to define where associated records such as audit trial information, embedded comments and time stamps may be found and how they are controlled. This process requires a procedure in lieu of any system checks. The procedure should define how the master is controlled and how the records, once printed out for hand written approval, are controlled to prevent their change, along with the process for approving the paper copy.

If the record is made up of multiple components of electronic and paper e.g. a batch record containing electronic weight records and paper records from chart recorders there should be a procedure to describe the management and approval of these components.

Another example is a laboratory data recording system. This uses a proprietary spreadsheet package, which is used to perform calculations. These systems currently do not support electronic signatures and audit trials compatible with 21 CFR Part 11. The report has to be printed out and signed. The system does not support a time-stamped audit trail of operator entries and actions that modify or delete the master record. A standard operating procedure has to be used to describe the process of controlling the master record once approved, and for logging all changes to it.

6.4.5 CONTINUOUS PERIODS OF USE

The regulation requires only one part of the two component signature to be entered during a period of continuous use, the operator having successfully logged in initially with both components.

A ‘continuous period of use’ requires that the operator physically remain at the screen. If the operator leaves the room to take a sample or go for shift breaks then this is not a continuous period of use and will normally require logging off and then logging back on using both components of the signature. However, another permitted option is to put the screen into a secured pause state on leaving and then using a controlled access re-start on return. This process should be documented in an operating procedure. If a system is in continuous use round the clock and the operator is not always at the terminal then any entry of an electronic signature requires the entry of both signature components. There should be a specification of the activities where a formal electronic signature is required by the system.

An example is a plant process control system, which is operating 24 hours per day providing control functions, monitoring the plant and recording batch data as an electronic record. The operator may not always be in the control room so

the system should provide functionality to apply electronic signature as a two component action when required according to pre-defined specifications. Examples of when electronic signatures apply are given in 6.4.1.

6.4.6 DEVICE CHECKS

There are two types of device check, automated and manual.

Typical device checks can include device type, device identity, device status (e.g. calibrated), and device location. Such checks can be used where appropriate to accept or reject the device as a valid source of data. Typical examples are:

- A weighing machine of the correct type (e.g. range) and in calibration is connected to the system
- Approval of a raw material should be transmitted only from PCs within a designated QA area
- A batch material picking list is sourced from a terminal within the Material Planning Function

Such checks can be automatic if the system has the functionality to make these checks, alternatively such checks can be achieved by physically checking the device type and its installation records/connection, for example during IQ.

6.4.7 OPERATIONAL SYSTEM CHECKS & AUTHORITY CHECKS

In some systems, it may be possible and sensible to build in checks to enforce a particular operations sequence and a particular authority. An example is a workflow driven Electronic Document Management System, which enforces a permitted sequence of operational steps in a specified order, e.g. forcing the review of a document before its approval, and approval before issue. During these operational steps, authority checks are performed by the system to ensure that only specified individuals are able to perform the operation (e.g. document approval).

These types of checks are clearly an important and sensible requirement of such a system. Such functions can be clearly specified, designed, tested, and accepted as part of the system specially written for operation in a GMP environment. For other systems particularly more general data gathering systems it may not be possible or sensible to build such functions into the system and any required operational sequence checks or authority checks for GMP reasons will have to form part of standard operating procedures.

6.4.8 USE OF CURRENT E-MAIL TECHNOLOGY

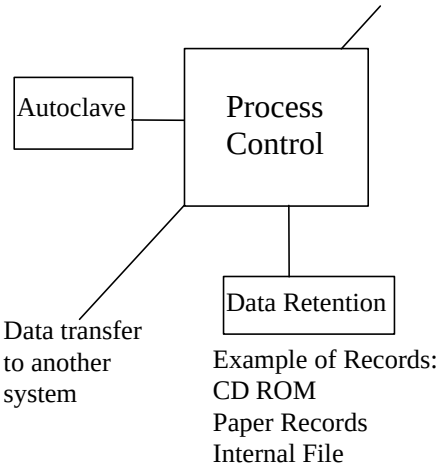
E-mail is a flexible communications tool used by many people to send messages, notes, and documents.

The validation of such systems poses fundamental problems around the lack of audit trails, administration, robustness, and security, particularly with data passing from open to closed systems. Due to these problems, an e-mail cannot be considered to be a secure electronic record. It should not be used for transmitting authorisations, capturing GMP data, or transmitting approved master documents.

6.5 APPENDIX 5 – EXAMPLES OF APPLYING 21 CFR PART 11

PROCESS CONTROL SYSTEM

Diagram



Description

Process control system is used to control and monitor critical parameters. There is user interaction to initiate the progress and respond to alarms. Data from the system can be retained. Alternatively data can be transmitted without retention to another system/equipment.

User Interface Examples:
Panel, display, PC, monitor.

Critical Parameters Examples:
Temperature, pressure, time.

Electronic Records and Signatures

Electronic Records Are
Any retained data
e.g. on CDROM, Internal Files

Electronic Signatures Are
Any approvals made electronically required for GMP (e.g. sequence stages of an electronic batch record).

Notes: If the data is transmitted to other system/equipment without use of internal files then this does not constitute an electronic record.
Hybrid System: It is very likely that on existing systems the batch record is printed and approved by hand-written signature . (See section 6.4.4.)

Issues to Manage

-Password & user ID Management
-Transfer of Retained Data
-Unlikely to have associated audit trail.
-Hybrid System.
-Internal File may be over written.
-(E.g. on a rolling basis)

SPREADSHEETS

Diagram

- Manual data input

User Interface

PC

Application and Calculation

Data Retention

Examples:
Files
Paper
Electronic Storage

Automatic Data Transfer

Description

PC with standard application package with local calculations and macros generates data which is retained and used to support GMP.

Electronic Records and Signatures

Electronic Records Are
Any spreadsheets containing GMP data.

Electronic Signatures Are
Typically none even though they are needed

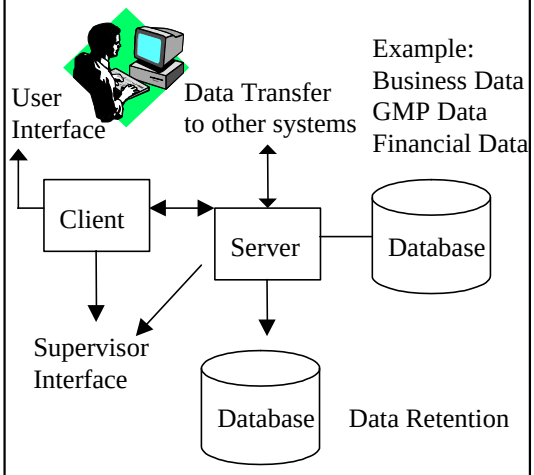
Issues to Manage

-No control
-No audit trials
-No access controls
-Volume of data

Consider creating a signed off copy by manual review and approval. Apply procedural controls, including manual audit trail.

MRPII

Diagram



Description

MRP II Systems are used to manage material and production management. Provide user interface to material and product identification e.g. barcodes and status. Used to creation and maintain bills of materials and to schedule batches. Large amounts of data are managed and retained.

Examples of Storage Media Include:
Internal Files
Tape, Disk, CD Storage
Paper
Microfiche

Electronic Records and Signatures

Electronic Records Are
Table of GMP relevant items from GAMP 3 Vol 2, Section 3.9

Electronic Signatures Are
Should be used for all Approvals/authorisations

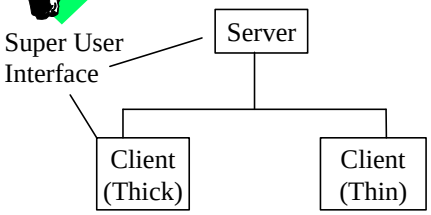
Issues to Manage

-Audit trail file
-Password File
-User Profile
-Long term retention of data
-Hybrid Systems
-Insertion of signatures may not be possible
-Super Users.
-Volumes of data to archive e.g. audit trails information.
-Link to desktop and networks.

DESKTOP

Diagram

Desktop
Client/Server/PC/Network



Description

Provides infrastructure support to network applications, with secure access to data and data management. Supports user access to applications.

Organisation rely on infrastructure for: access control and security; backups; virus controls; deployment of s/w fire wall. The network is a public domain

Network Examples:
Local
Wide

Example of Clients running applications:
Windows PC
Macintosh
NetPC

Electronic Records and Signatures

.

Electronic Records Are
- User access control records,
- installation/deployment records
- configuration management records
- qualification records of electronically updated software

Electronic Signatures Are
None. Signatures are applied from within specific applications which are accessed via the network.

Issues to Manage

- Management of user profiles and authority.
- Role and authority of super user.
- Deployment of software for validated applications in regulated environment.
- Configuration management.
- Conflicts between applications on clients.
- Thin/Thick clients.
- Timeouts of clients.
- Password management.
- Virus management.

Laptops - transport of data

Chromatography Data System

Diagram

User Interface

ChromeBox

Data System

Data Retention

Data transfer to another system

Example of Records:
CD Rom
Paper Records
Internal File

Description

Chrome box acquires data plus set up & base line information. The Data System stores and processes data draws a graph and calculates area. Data from the system may be retained Alternatively data can be transmitted to another system (e.g. LIMS) for long term retention.

Hard copy may be printed off for signature

PC retains data for recalculation

Electronic Records and Signatures

Electronic Records Are

Any retained data
e.g. on CD Rom, Internal Files

Electronic Signatures Are

Any approvals made electronically required for GMP

Notes : data may be transmitted to other system without use of internal files then this does not constitute an electronic record in the CDS, but may be elsewhere.

Hybrid System : It is very likely that on existing systems the graph is printed and approved by hand-written signature .

Issues to Manage

-Password & user ID
-Transfer of Retained Data.
-May not have associated trail.

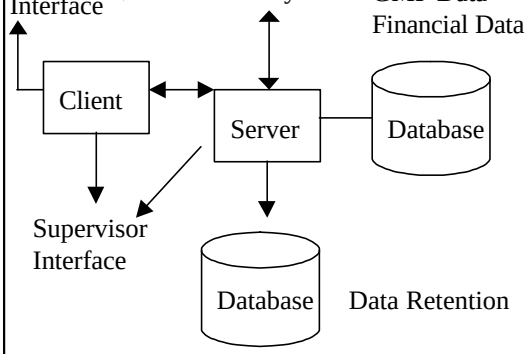
-Hybrid
-Internal File may be over
-E.g. on a rolling basis

-Long term data storage in a portable data

-Raw or original data that requires safe secure archival includes all the set-up and baseline adjustment data.

Electronic Document Management System (EDMS)

Diagram



Description

EDM Systems are used to manage compliance and manufacturing documents. The system managers documents through the life cycle. (See appendix 7.)
Large amounts of data are managed and retained.

Examples of Storage Media Include:
Internal Files
Tape, Disk, CD Storage
Paper
Microfiche

Electronic Records and Signatures

Electronic Records Are
Documents, attributes (metadata).

Electronic Signatures
Should be used in accordance with Section 6.4.1.

Issues to Manage

-Audit trail file
-Password File
-User Profile
-Long term retention of data
-Hybrid Systems
-Insertion of signatures may not be possible
-Super Users.
-Volumes of data to archive e.g. audit trails information.
-Link to desktop and networks.

Document Management Systems fall into two broad categories. The first group of systems accept electronic documents as input and manage these electronic documents throughout the document's life cycle. These documents may be SOPs, reports, change control documentation, batch records, or any type of document that must be maintained for a defined period. Some systems use electronic signatures for approval, while some use the hybrid approach, where a hand written signature is used to authenticate an electronic document. Whether or not they use electronic signatures, this type of Document Management System must comply with the requirements for electronic records. If electronic signatures are used, they must comply with the requirements for electronic signature.

The second category of Document Management System is designed to manage documents that are scanned in from a paper original, such as a Case Report Form or other document. In many cases, the paper document is the original reference, and the scanned copy is simply a facsimile. If the original paper document is maintained and archived as the original record, and the computer system is storing the electronic images for internal management purposes only, that computer system does not need to comply with the requirements for electronic records.

6.6 APPENDIX 6 - FDA COMPLIANCE POLICY GUIDE; ENFORCEMENT POLICY: 21 CFR PART 11

Office of Regulatory Affairs
COMPLIANCE POLICY GUIDE Section 160.850

COMPLIANCE POLICY GUIDE

Section 160.850

Title: Enforcement Policy: 21 CFR Part 11; Electronic Records; Electronic Signatures (CPG 7153.17)

Background:

This compliance guidance document is an update to the Compliance Policy Guides Manual (August 1996 edition). This is a new Compliance Policy Guide (CPG) and will be included in the next printing of the Compliance Policy Guides Manual. The CPG is intended for Food and Drug Administration (FDA) personnel and is available electronically to the public. This guidance document represents the agency's current thinking on what is required to be fully compliant with 21 CFR Part 11, "Electronic Records; Electronic Signatures" and provides that agency decisions on whether or not to pursue regulatory actions will be based on a case by case evaluation. The CPG does not create or confer any rights for or on any person and does not operate to bind FDA or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statute, regulation, or both.

In the Federal Register of March 20, 1997, at 62 FR 13429, FDA issued a notice of final rulemaking for 21 CFR, Part 11, Electronic Records; Electronic Signatures. The rule went into effect on August 20, 1997. Part 11 is intended to create criteria for electronic recordkeeping technologies while preserving the agency's ability to protect and promote the public health (e.g., by facilitating timely review and approval of safe and effective new medical products, conducting efficient audits of required records, and when necessary pursuing regulatory actions). Part 11 applies to all FDA program areas, but does not mandate electronic recordkeeping. Part 11 describes the technical and procedural requirements that must be met if a person chooses to maintain records electronically and use electronic signatures. Part 11 applies to those records required by an FDA predicate rule and to signatures required by an FDA predicate rule, as well as signatures that are not required, but appear in required records.

Part 11 was developed in concert with industry over a period of six years. Virtually all of the rule's requirements had been suggested by industry comments to a July 21, 1992 Advance Notice of Proposed Rulemaking (at 57 FR 32185). In response to comments to an August 31, 1994 Proposed Rule (at 59 FR 45160) the agency refined and reduced many of the proposed requirements in order to minimize the burden of compliance. The final rule's provisions are consistent with an emerging body of federal and state law as well as commercial standards and practices.

Certain older electronic systems may not have been in full compliance with Part 11 by August 20, 1997, and modification to these so called "legacy systems" may take more time. As explained in the preamble to the final rule, Part 11 does not grandfather legacy systems and FDA expects that firms using legacy systems will begin taking steps to achieve full compliance.

Policy:

When persons are not fully compliant with Part 11, decisions on whether or not to pursue regulatory actions will be based on a case by case evaluation, which may include the following:

Nature and extent of Part 11 deviation(s).
FDA will consider Part 11 deviations to be more significant if those deviations are numerous, if the deviations make it difficult for the agency to audit or interpret data, or if the deviations undermine the integrity of the data or the electronic system. For example, FDA expects that firms will use file formats that permit the agency to make accurate and complete copies in both human readable and electronic form of audited electronic records. Similarly, FDA would have little confidence in data from firms that do not hold their employees accountable and responsible for actions taken under their electronic signatures.

Effect on product quality and data integrity.
For example, FDA would consider the absence of an audit trail to be highly significant when there are data discrepancies and when individuals deny responsibility for record entries. Similarly, lack of operational system checks to enforce event sequencing would be significant if an operator's ability to deviate from the prescribed order of

manufacturing steps results in an adulterated or misbranded product.

Adequacy and timeliness of planned corrective measures. Firms should have a reasonable timetable for promptly modifying any systems not in compliance (including legacy systems) to make them Part 11 compliant, and should be able to demonstrate progress in implementing their timetable. FDA expects that Part 11 requirements for procedural controls will already be in place. FDA recognizes that technology based controls may take longer to install in older systems.

Compliance history of the establishment, especially with respect to data integrity. FDA will consider Part 11 deviations to be more significant if a firm has a history of Part 11 violations or of inadequate or unreliable recordkeeping. Until firms attain full compliance with Part 11, FDA investigators will exercise greater vigilance to detect inconsistencies, unauthorized modifications, poor attributability, and any other problems associated with failure to comply with Part 11.

Regulatory Action Guidance:

Program monitors and center compliance offices should be consulted prior to recommending regulatory action. FDA will consider regulatory action with respect to Part 11 when the electronic records or electronic signatures are unacceptable substitutes for paper records or handwritten signatures, and that therefore, requirements of the applicable regulations (e.g., CGMP and GLP regulations) are not met. Regulatory citations should reference such predicate regulations in addition to Part 11. The following is an example of a regulatory citation for a violation of the device quality system regulations.

Failure to establish and maintain procedures to control all documents that are required by 21 CFR 820.40, and failure to use authority checks to ensure that only authorized individuals can use the system and alter records, as required by 21 CFR 11.10(g). For example, engineering drawings for manufacturing equipment and devices are stored in AutoCAD form on a desktop computer. The storage device was not

protected from unauthorized access and modification of the drawings.

Issue date: 5/13/99

6.7 APPENDIX 7 – ELECTRONIC DOCUMENTS AND THEIR MANAGEMENT LIFECYCLE

6.7.1 ACKNOWLEDGEMENTS

This Appendix has been produced from information developed by the following members of the GAMP Special Interest Group on Electronic Records and Signatures:

Leif Poulsen (Main Author)
Rob Almond
Heinrich Hambloch
Gert Mølgaard
Peter Robertson
Kate Samways
David Selby
Caroline Smith
Sion Wyn

6.7.2 INTRODUCTION

The purpose of this Appendix is to provide guidance on best practice surrounding the management of electronic documents found in pharmaceutical manufacturing, such as Standard Operating Procedures, Batch Records, Laboratory Analysis Reports, and Deviation Reports. It is aimed at system owners, implementers, and users in production, engineering, quality assurance, and information management.

The major sections of this appendix are:

- The Document Lifecycle – the activities and stages through which a document passes during its existence
- Types Of Documents – how documents may be stored electronically

6.7.3 THE DOCUMENT LIFECYCLE

Documents have their own life cycle ranging from the initial idea of the document to the destruction of the document when it has no further purpose. This section describes a typical document life cycle model as applied in the pharmaceutical industry (see Figure 6-1).

For each step in the life cycle, the document is subject to a number of activities that may be classified as main or support activities.

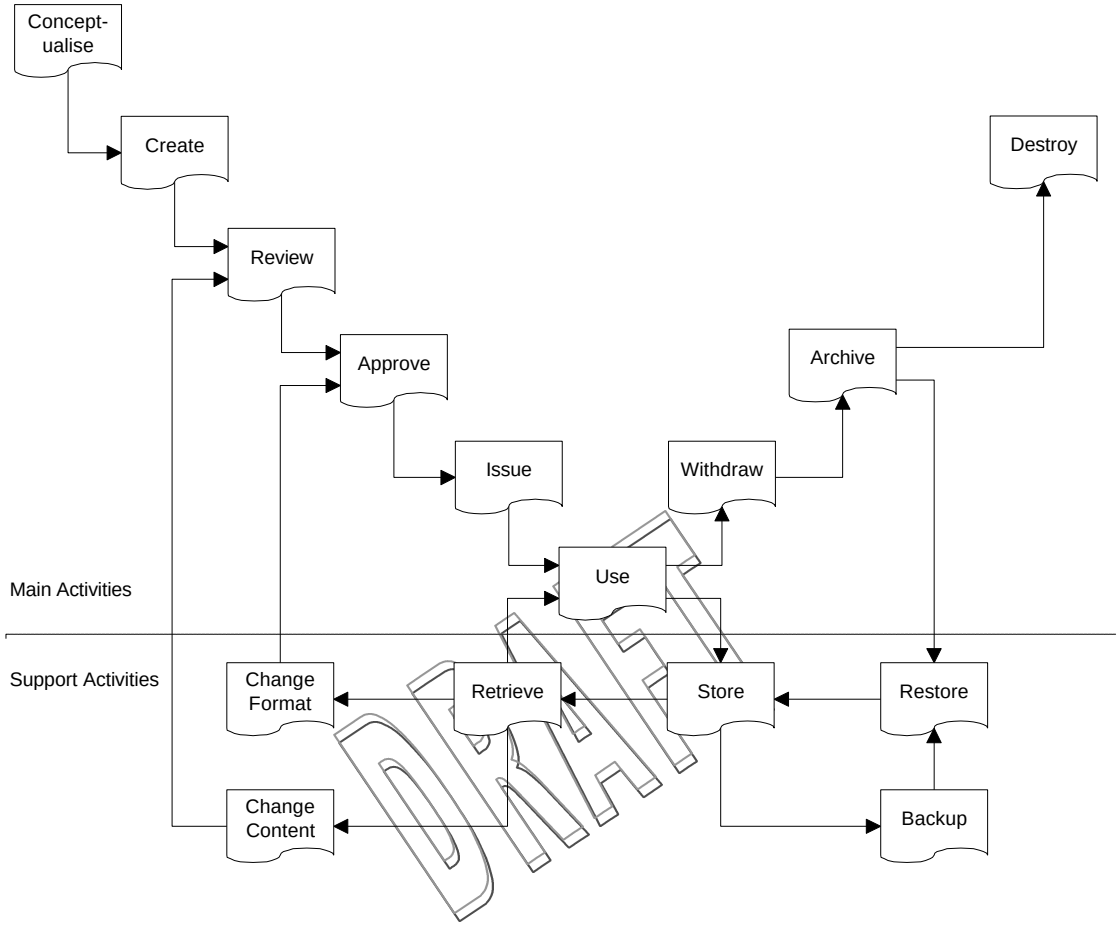


Figure 6-1. The Document Lifecycle

6.7.3.1 Main Activities

a) **Conceive Document.** Before creation of the document, an idea of the purpose and scope of the document must exist as well as definition of the author, reviewers, and approvers. This will have an impact on the choice of structure and format of the document, e.g., it must be decided if the document should be a pure text document or if it should comprise graphical objects. A version control process will be proposed and the implications of

existing guidelines or SOPs taken into account. At this stage, it will be helpful to consider the handling of electronic signatures and the definition of access authorisations for use.

b) **Create Document.** The document is created in an electronic version typically by use of traditional desktop applications either from scratch or by copying/scanning parts from existing documents. In any case, the application used must be defined, including version. The document comes into existence by assigning a unique identification number and a version number. Storage location and back-up procedure should be considered. The document status is set to "**Draft**".

c) **Review Document.** Before approval and use of the document, it must be checked for errors, consistency, and completeness during one or several formal or informal reviews. The appropriateness of style and whether the content is at the right level for understanding should be included in checks. For each discrete review the version number must be updated. The document status is still at "Draft".

d) **Approve Document.** Upon final review, the document will be sent in a workflow for approval. Normally this involves several categories of people, e.g. approval of master recipes involves both process engineers and QA. The approval of the document may be performed using an electronic signature. Upon approval by the last person in the workflow the document status is changed to "**Approved**".

e) **Issue Document.** Now the document may be distributed to identified recipients for use. However often this must be preceded by some additional indexing (e.g. adding of extra search keys) and formatting (e.g. transfer to read-only format) performed by the document controller. A document owner and storage location will have been nominated. The document status is then changed to "**Released**".

f) **Use Document.** In some cases the approval step is associated with setting an "Effective from date", which must be reached before the document may be used. By reaching this date the document status is changed to "**Effective**" and may be taken into use. Print enabling may occur here if previously restricted.
Throughout this phase, the document is readily available to all those who may need to refer to it and is subject to formal change control processes and access security measures.

g) **Withdraw Document.** Any document may become obsolete and may then be replaced by another document or another version of the same document. Only one version of a document may be effective at a time. Old versions must be withdrawn whenever the "Effective from date" of the replacement document has been reached. The status of the superseded version is then changed to "**Withdrawn**". Document users may need to be informed of the change.

h) **Archive Document.** After withdrawal of a document, it may be archived on a long-term storage media, e.g. tape or jukebox. Many document types in the pharmaceutical industry have to be kept for many years; a retention period of 10-20 years is quite normal. This requires careful configuration management of all necessary retrieval and access tools that have to be archived along with the document. More than one copy may be needed for security.

i) **Destroy Document.** Upon completion of the required retention period, the withdrawn document may be removed from the long-term archive and deleted such that it can no longer be retrieved for any purpose. It is important for GMP reasons to ensure all copies are destroyed, with a record of the date of destruction and proof to that effect.

6.7.3.2 Support Activities

a) **Store Document.** Upon any change of a document, a copy has to be stored on an on-line medium.

b) **Retrieve Document.** Any use of an electronic document must be preceded by a retrieval process, which may be helpfully facilitated by having the appropriate search key and search functions available.

c) **Backup Document.** For security reasons a copy of every document version has to be kept on a safe medium, e.g. tape or jukebox.

d) **Restore Document.** Documents kept on archive/backup media have to be restored to an on-line media before they can be used.

e) **Change Document Format.** Document formats may have to be changed due to migration from an old version of a software package to a newer version. As described below proper document management has to be associated with proper system configuration management.

f) **Change Document Content.** The document content may have to be changed for various reasons. Any change has to be controlled by a change management system. This will often require creation of a change request, which has to go through its own approval workflow before the change can be implemented in a controlled document. In order to prevent two persons from changing the same document simultaneously document management systems normally support document check-out/check-in.

6.7.3.3 Document Structure

A pre-requisite for proper document management through all life cycle phases is a systematic approach for indexing the document.

Each document must have a unique identification consisting of:

- Document Number
- Version Number

Further, the document normally has to be assigned with a set of more descriptive attributes for facilitating the document management. Typical attributes include:

- Document Title
- Author Name(s) or Initials
- Owner Name or Initials
- Approver Name(s) or Initials
- Approval Date
- Issue Date
- Effective Date
- Withdrawal Date
- Current Status
- Replaces……..
- Language
- Minimum storage time

("Replaces" is a reference to a previous version of the document and is important for establishment of the necessary audit trail.)

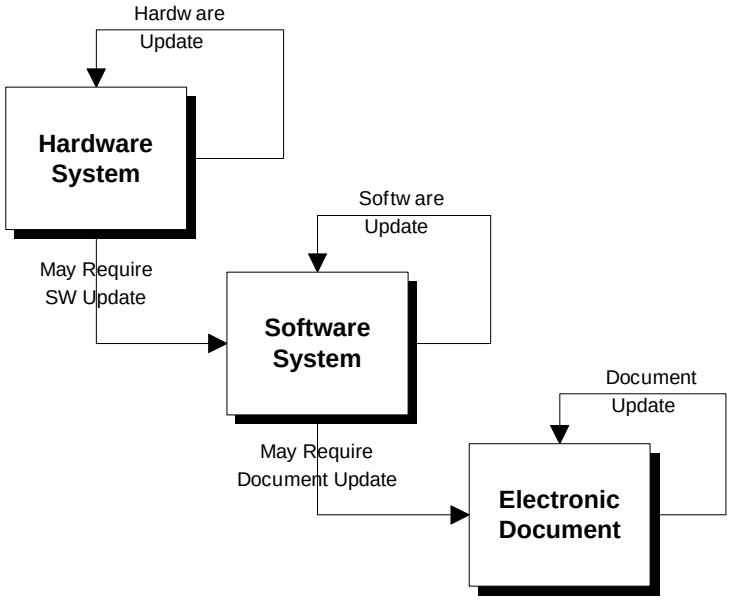
6.7.3.4 Document Status

Some of the activities in the life cycle model may change the current status of the document. The following document states are often used:

- Draft (the initial state from creation till approval of the document)
- Approved (from approval by QA to release by document control)
- Released (from release by document control till effective date is reached)
- Effective (from effective date to withdrawal by document control)
- Withdrawn (from withdrawal to destruction of document)

6.7.3.5 System Life Cycle

The life cycle of electronic and paper-based documents may be very similar, however electronic documents can only be handled by systems comprising hardware and software, which have their own life cycles as, outlined in the figure below. Any change in the set-up of hardware and software may thus require updates of the electronic document. A typical example is upgrading of document reader software from an old (no longer supported) version to a new version, resulting in the need to produce a new electronic copy of the electronic document, which is compatible with the new reader software. This illustrates that proper management of electronic documents is closely related to proper system configuration management.


Hardware Update
Hardware System
Software Update
May Require SW Update
Software System
Document Update
May Require Document Update
Electronic Document

6.7.4 TYPES OF DOCUMENTS

Documents in a pharmaceutical company include a range of types which are of quite different natures, spanning from complex compound documents over traditional text documents down to sets of raw data e.g. from data collection on a batch. As the whole range of documents is subject to regulatory requirements and quality requirements, each document needs to be dealt with rigorously in the document management system.

The generic requirements are not complicated, but in the rapidly evolving electronic world new document management facilities and software functionality does lead to some complexities that need special caution.

Best practice is to store the information relating to the source of the document (e.g. product and version) together with the document itself. This should include information on not only the creator, approver etc. of the document but also its technical source, including, for example, the word processing package including its version. For more complex data types, this may be complicated since a compound document of text, graphics, spreadsheet, tables etc. may have several sources. However, if dynamic linking between documents is avoided so that all sub-parts of a compound document are embedded into the document, it may be sufficient to record the technical source of the main document itself and leave the more detailed source descriptions to the configuration management system of the overall environment.

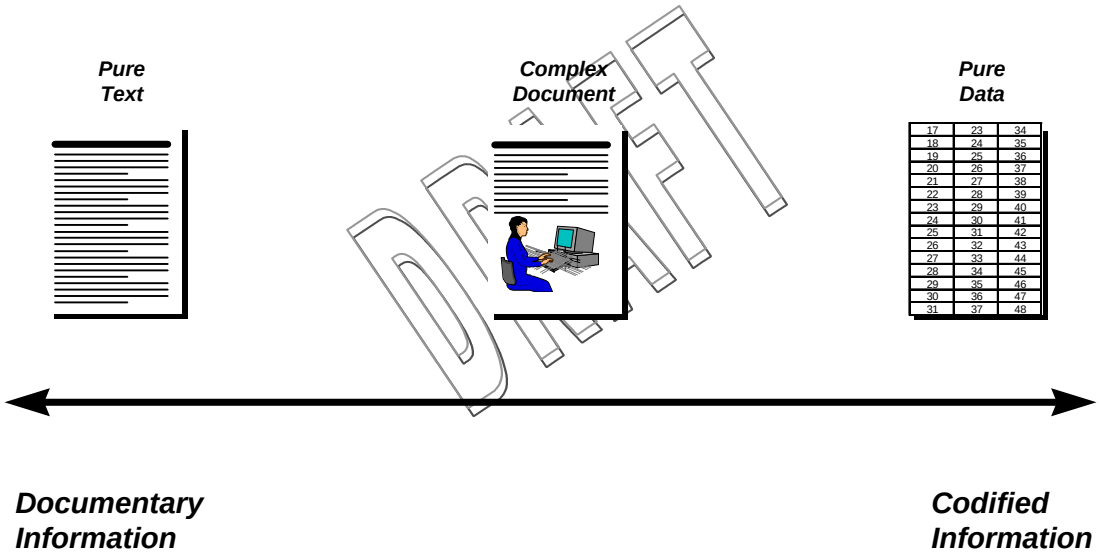
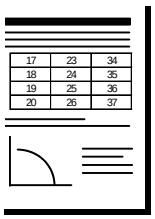
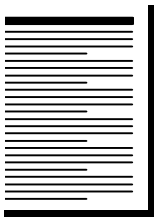
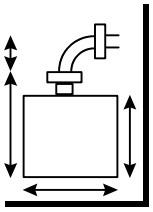
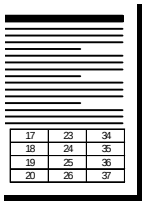
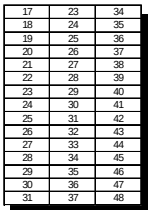


Figure 6-2. The Continuum of Document Types

Figure 6-3. Characteristics of Various Document Types

Document type	Characteristics	Examples of Application areas	Special Precautions
Portable format document 	A homogenous document type created from any other type of documents, but stored in a standard or proprietary file format. The international standard format is SGML. Several proprietary formats exist of which Adobe's PDF format is currently popular. A semi-portable file format is HTML, which is used on the Internet World Wide Web. See also the compound file formats. Files can typically not be edited in this format, but can be created from most other types The programs normally require a graphical user interface (GUI).	All document types including more complex such as integrated batch documentation, illustrated SOP's, all document types to be stored in a 'neutral' file format.	Specify file format, application and version. Control of printer drivers may be necessary
Pure Text Document 	The simplest document type to manage. Typically, a text file created in a word processor, which consists of pure text and in which all of the document can be viewed by the word processor program itself or a file viewer program. Simplest file format is ASCII or ANSI files. Many proprietary formats exist but the most popular have become de-facto standard formats.	Memos, master production and control records, SOP's, deviation reports, validation protocols, manual batch documentation and many more	Specify file format, application, version and language

Document type	Characteristics	Examples of Application areas	Special Precautions
Graphical Document 	A homogenous document type, stored in a standard graphical file format. Includes scanned paper documents. Many file formats exist from raw bit-mapped pictures to highly complex vectored drawings in a CAD environment. Simplest file formats are bit-mapped formats (e.g. TIFF, PCX, GIF, JPEG) or generic vectorized formats (e.g. WMF, CGM, DXF). Many proprietary formats exist. Some CAD formats include product database information.	CAD drawings, SOP illustrations, scanned paper documents, label pictures for batch documentation.	Specify file format, application, version and language
Complex Document 	A non-homogenous document type consisting of elements of a different nature, e.g. text and graphics, tables etc. that are created or imported into one homogenous file format. File formats are typically one of the proprietary word-processor formats of which the most popular have become de-facto standards	Word processor documents with figures, graphs etc.	Specify file format, application and version. May require specification of format, application and version of the embedded elements
Compound Document 	Most of the most modern documents consisting of document objects, which are separate 'files' based on proprietary or industry standard object models (e.g. OLE, OpenDoc). The objects may be textual, graphical, data-based etc. Compound formats also include HTML documents (the Internet WWW format) in which the graphical elements etc. are stored separately.	All types of documents created with a newer version of all office application suites.	Specify file format, application and version. May require specification of format, application and version of the embedded elements May even require specification of operating system

Document type	Characteristics	Examples of Application areas	Special Precautions
Pure Data Document 	Structured files or databases with raw data, which can be interpreted only by program for the specific purpose. File formats include structured raw text files (e.g. comma separated ASCII or ANSI files, CSV, DIF), several proprietary database formats (eg. dbf, db, mdb) and strictly proprietary formats in a binary format, which can be interpreted only by the proprietary program.	Laboratory sample tables, process control trend curves, In Process Control sample tables, all kinds of database applications.	Specify application and version

6.7.4.1 Portable file formats

All document types can be converted to ordinary flat files in a portable format through special programs, which create an electronic printout into a portable data format such as Adobe PDF, SGML, or Encapsulated PostScript. After conversion such documents cannot be edited or changed and thus provide a secure storage format which can be published and printed in a reliable format.

The regulatory bodies are presently working on guidelines on which file formats they accept or prefer for submissions. The different country/region preferences may be summarised into

- Europe: TIFF, ASCII some PDF
- US: PDF, TIFF, ASCII
- CAN SGML

A special portable file format is HTML, which has gained popularity through the widespread use of the Internet World Wide Web. The HTML format is not yet a publish-true format, as it does not guarantee the format of the document when displayed on different computers or when printed. It is, however, highly popular for publishing on the Internet or on corporate Intranets.

6.7.4.2 Pure text files

The simplest document types are those including only documentary information in a raw text file format. Most simple are *ASCII files* (or *ANSI files*) with no formatting information included, since they may be created, viewed, or managed with any word processor or computer editor. Such raw text documents are the easiest to manage since they are only little dependent on the technical environment, however they are less reader-friendly than formatted word processor documents, which has become much more popular. However, in an international environment the character encoding should be recorded, (e.g. ASCII or ANSI) as well as the character encoding of national characters (e.g. German, French or Scandinavian files in DOS or Windows, where it may be necessary to specify code page set-up for the screen and printer).

Word processor files are formatted files, where the formatting of the document and its file format depends on the type and version of the word processor. It may be necessary to use exactly same type and version of word processor to view or edit a document if it must be identical to the original.

Pure text documents is becoming less frequent as most modern word processors include the ability to link or embed different information types into the document, thus creating a non-homogeneous document of text, graphics, tables, sound etc. Textual documents may also be graphical documents creating by scanning into the computer system. Such documents are bitmapped images and cannot be edited or changed unless they are converted through OCR software into ordinary text files, that must be carefully verified.

6.7.4.3 Graphical Files

Graphical files can be either bitmapped or vectorized. In general, it is important to specify the application in which the graphical file is created. Some standard formats have gained broad acceptance, including tiff, pcx, jpeg, and gif for bitmapped files or cgm and wmf for vectorized. This is even more critical for CAD files, in which the proprietary file formats may include database information for the components in a drawing. The type and version number of the application are most important for most file types.

6.7.4.4 Complex documents

Complex documents are documents with imported parts from different sources embedded into one document. To ensure proper control of such documents the type and version of the application source of each part may need to be specified with each managed document.

6.7.4.5 Compound documents

Compound documents are documents with embedded parts (objects) from different sources, where each part can be in-line edited in the file. For these it may be necessary to specify not only the type and version for each application source but also of the operating system to ensure that the document is maintainable throughout its life cycle.

6.7.4.6 Raw data

Raw data are files or databases, which contain structured records of values. In its simplest form, it may be simple text files in a fixed record format or in a variable format with separating characters (e.g. comma separated ASCII files). However, this is a very inefficient storage form and therefore many raw data applications have developed proprietary data formats, which can be read only by the proprietary program. Many such applications have published their file format, thus enabling third party companies to interface to their proprietary files. For these file types, it is typically sufficient to record the application type and version to enable use and maintenance of the data files.

1. Special types of raw data files are the data files of relational database systems. For smaller database applications the data files may be handled like other types of files, but typically such data files are updated frequently and thus their management and use are a specialist subject. In these cases, Operating Procedures are required to define the processes for ensuring data integrity and security.

6.8 APPENDIX 8 - EXAMPLES FROM WARNING LETTERS

The following issues have been raised by the FDA in recent Warning Letters to pharmaceutical organisations:

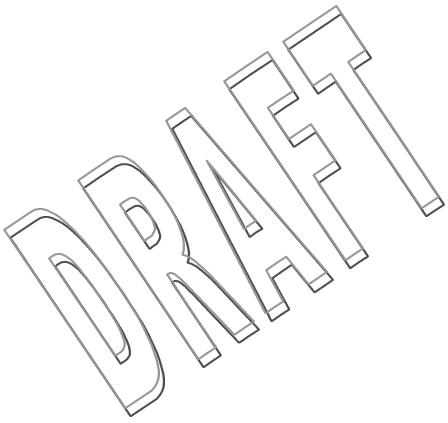
1. Lack of audit trail, with no way to determine if values had been changed on batch production records. The system in question only recorded the last value entered; any previous entries would not be known (including any out-of-range values).

2. No written procedures that would hold individuals accountable for actions under their electronic signatures.

3. No documentation or testing of the system's ability to discern invalid or altered records.

4. No documentation to show if the system has the ability to generate accurate and complete copies of records in electronic form.

5. No safeguards to prevent unauthorised use of electronic signatures that are based on identification codes/passwords when an employee who has logged onto a terminal leaves the terminal without logging off.



6.9 APPENDIX 9 – GLOSSARY

The following are terms as defined in 21 CFR Part 11.

Closed System	Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
Digital Signature	Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
Electronic Record	Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
Electronic Signature	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.
Handwritten Signature	Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate 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.
Open System	Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

6.10 APPENDIX 10 – REFERENCES

References to common document format standards, e.g. from FDA, to be included.