1. Purpose

The purpose of this document is to provide an interpretation of FDA 21 CFR Part 11, Electronic Records; Electronic Signatures (ER/ES) and to provide guidance for acceptable practices in the use of electronic records and electronic signatures by any site.

2. Scope

This guideline is directly applicable to any function, department, or site that operates to US FDA GLP, GCP and/or GMP standards, or that generates records or data that are submitted electronically to FDA. It will be useful in meeting the expectations of other regulatory authorities worldwide and so further references to GLP, GCP and GMP are not explicitly restricted to the FDA.

2.1 General

This guideline applies to any computerised system that creates, modifies, maintains, archives, retrieves or transmits records required by the predicate rules of GLP, GCP, GMP or submitted records, electronically in whole or in part in place of paper records.
It does not currently apply to systems that were in operation before 20 August 1997 and met the requirements of the predicate rules, provided those systems continue to satisfy the predicate rules despite changes made to their architecture or functionality. It also does not apply to systems which have their records transferred to paper for all regulated purposes.
It is applicable to any computerised system that uses electronic signatures in place of hand-written signatures but only for purposes of compliance with GLP, GCP, GMP or regulatory submission requirements.

2.2 Faxes

An ordinary fax is outside the scope unless it is generated or received by a computerised system which falls within the general scope.

2.3 Documents

Some documents which are principally text and do not contain ólive' data, such as SOPs, validation documentation, computer system documentation, laboratory test methods, deviation reports, etc. may be created using proprietary software, but used only on paper. In this situation the electronic version is not within the scope of ER/ES if the original electronic document is used only by the author for the sole purpose of creating a paper copy and only the paper copy is made available for general use. If the documents are required by predicate rules and are signed, maintained, distributed or otherwise made available electronically, ie the electronic version is *used for regulated purposes,* then they become electronic records within the scope of ER/ES. Note that the risks associated with their use, particularly if ór ead-only', should be considered in defining the approach to take. A validated document management system is nonetheless the preferred way to achieve a compliant state for these documents (see Section 5.4.1).

3.7 Hand-written Signature Maintained Electronically

A traditional hand-written signature written on a paper record that is later scanned into a computer system and thus becomes an electronic representation of the original record.

3.8 Hybrid System

A system that produces both electronic and paper records, each of which may be used for a different purpose (e.g. electronic batch record system from which paper batch records are printed and used for manual data collection). It can also be a system where a printout from an electronic record is authenticated by a hand-written signature.

3.9 Non-biometric Electronic Signature

An electronic signature that is executed by the use of at least two distinct identification components such as an identification code (i.e. User ID) and password.

3.10 Open System

An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

3.11 Access

The authority and ability to create, delete, modify, administer or read electronic records.

3.12 Metadata

Metadata describes the context and content of records, or otherwise further defines their structure and management through time.

3.13 Transient Data

Data stored temporarily in files that are passed as part of normal workflow on to a printer or other system before the process task is complete. Transient data with regulatory uses will generally only be stored on a local hard drive which should not be readily accessible and is automatically overwritten when a short term pre-set limit is reached or the store is filled, whichever occurs first.

4. Responsibilities

Each responsible QA organization should ensure that its associated site or function with records in the scope of this Guideline has procedures in place to ensure that this Guideline is met.

System Owners are ultimately responsible for ensuring that new systems accepted by them, or existing systems in their ownership, comply with those procedures and remain in compliance throughout their lifecycle. Many of the specific activity responsibilities associated with this will commonly be delegated.

- A value (or record) outside acceptable ranges for the proper functioning of the computerised system
  This would be an invalid record, and the application should detect this and not accept the record (Note: if the record is outside the acceptable range defined for the business process the application may accept the input but issue a warning or similar message to alert to a potential error).

- A value with an unrecognisable data type
  This would be an invalid record, and the application should not accept the record. The system needs the ability to detect any corrupt or unrecognisable data.

- A value which is a result of a read operation which has a read error
  As above, the system needs the ability to detect any corrupt or unrecognisable data.

Altered records include those records where data has been added, modified, or deleted. The ability to view the detail of alterations to records is normally provided by the systemôs audit trail.

In some cases, particularly where critical data entry is involved or there is a predicate rule requirement for the ability to see immediately within a record that the record has been changed, it will be applicable to implement more stringent controls than an audit trail alone to fulfill this requirement.

If an audit trail alone is used, the representation of a changed record as an original record must be avoided by the following conditions:

- The audit trail must contain all required elements
- The audit trail must be searchable by record
- The audit trail must be in human readable form that is understandable to the operator of the system

Note: Other specific design considerations are conveyed throughout this guideline (e.g. audit trail- 5.2.3; electronic signature capability- 5.3).

5.2.3 Audit Trails

Any requirement for an audit trail will be defined by the relevant predicate rule but also by the need to be able to assure the trustworthiness and reliability of a record. The latter will vary according to the potential for impact on patient safety/product quality and a decision on the course to be taken should be *justified and documented in a risk assessment*. Note that the course of action can include physical and procedural measures ie. manually created and maintained logs, as well as logical security measures, again depending on the level of risk involved. Particular consideration should be given when users have to create, modify or delete regulated records during normal operation.

System level logs (and similar) are generated for most systems. These are activity logs typically at the operating system level that track activities such as logons/logoffs, changes to security settings, system shutdown/startup, and the like. This is different from the electronic record audit trail, which is generated at the application level and logs users actions performed to a specific electronic record. The low level of inherent risk in these system logs suggests

5.2.7 Security

If records are maintained electronically, there should be assurance that only authorised people can access the systems and authority checks should be built-in such that individuals can only perform functions within the system for which they have authorisation. Controls should include the following:

- Appropriate system and procedural controls over user IDs and passwords in order to protect against unauthorised access to system records, operations, or input/output devices.
- Procedures to clearly indicate the groups of users who may use the system, electronically sign a record, alter a record or perform other tasks related to the system.
- Technical architecture that includes safeguards against and facilitates the detection/monitoring of, unauthorised system use.
- Procedures for system administration that address access privilege granting/retracting and the periodic review of authorisations. System-specific SOPs or Operations Manuals should address the administration of internal security hierarchies within the system.
- Group access only available for read-only accounts.

System administrators routinely require privileges above and beyond those that are granted to users. Although it is recognised that the capability to intervene at any level in a system is likely to exist, those with this capability must be limited in number and identified, with documented evidence of their competence made available. In addition, evidence of change control of system and records together with an audit trail, system generated where feasible, should be kept. Access should be through an account that can be associated with an individual.

The use of generic, highly privileged accounts, such as "sysmgr" should be avoided wherever possible. Actions done under such an account must be well documented and justified.

5.2.8 Personnel Qualifications

Any staff who use, develop, or maintain a computerised system which includes electronic records or signatures should have adequate education, training, and experience to perform their job.

Documentation of suitability for a role is considered a GXP activity and any electronic records of such, if maintained electronically, should comply with the principles of ER/ES requirements, although in this context the risk associated with the records is considered low.

5.2.9 Open and Closed Systems

Open systems by their nature have greater security challenges than closed systems, and therefore require more stringent controls in order to comply with the regulation. Careful

either as part of a document or linked to a document.. It is also possible to sign a paper document and later scan the signed copy into a computer system. In most cases, it is necessary to link this signed page with a larger document that is also stored electronically.

In either case there should be linkage between the signature and document, and system controls should be such that the signature cannot be cut or copied from the record or pasted into the record. There should also be controls to either prevent a signed document from being changed after signing or to clearly indicate that the document has been changed. Such hand-written signatures maintained electronically should not be confused with true electronic signatures, although both can have the same legal significance.

Non-biometric electronic signatures are executed by entering a User ID and password. If the operator is at the computer for a continuous time period, electronic signatures may be executed by entering only the password for each signing.

The requirement for entry of User ID and password is satisfied during the initial logon to the system and it is possible to consider this an electronic signature, so that a password alone can subsequently be used for signing, if other requirements are met. In particular these should include controls to prevent impersonation such as remaining in close proximity to the workstation, inactivity auto-delogging and strict password security.

In order to assure that the individual was continuously at the computer, there should be controls in place such as automatic time-outs or other appropriate measures. If operator activity is not continuous then each signing should be performed by entering both the User ID and password. This may be the case if the operator leaves the computer between entries to perform other functions.

5.3.3 User ID and Password Controls

The nature of non-biometric signatures is such that strict controls are necessary to ensure their integrity and authenticity. In order to ensure that an electronic signature can only be executed by a unique individual there should be a policy that User IDs should be unique and never reused or reassigned to another person. If the system is accessible over the company wide area network, the combination of User ID/Password needs to be unique across the entire company. If, however, the system is, for example, only accessible within a siteôs local area network the uniqueness need only be proven within the coverage of that network.

The identity of an individual should be established upon issuance of a new User ID. A procedure should be in place to ensure that access is requested and authorized appropriately and that when a person leaves a department or changes responsibility their security authorisation is re-examined. Similarly, when a person leaves the site their account should be disabled immediately upon termination. Lists of users and their security levels should be periodically reviewed to ensure that only authorised staff have access to computerised systems.

Password control is also crucial for non-biometric electronic signatures. It is essential that the password be known only by the individual who owns it. System managers, owners, vendors, or other technical staff may have the ability to reset the password in the event that it is forgotten or compromised but password maintenance by a userôs peer or colleague is not an acceptable practice. When an individual forgets their password it should be necessary to establish the identity of the person prior to resetting it. Upon first use of a newly issued or reset password the system should force the user to change to one known only to them. For

including possible disciplinary action, may be necessary. If the violation was outside of the personôs control, then the cause of the violation should be addressed in order to prevent recurrence.

5.3.7 Individual Certifications

For systems that utilise electronic signatures, each user of the system who will execute an electronic signature must sign a certification declaring that his/her electronic signature is the legally binding equivalent of his/her hand-written signature, prior to being granted the authority to perform electronic signings. This serves to confirm that the signer accepts the significance of the electronic signature, besides being a specific regulatory requirement. There should be documented training of these individuals to indicate that they understand the significance of the certification.

This certification need not be submitted to FDA, but should be retained and available in the event of an FDA or other authority request.

5.4 Interpretation for Specific Types of Systems

While general guidance is included in this document for the use of electronic records and electronic signatures, specific guidance is given here for various classes of computer systems.

The guiding principle in arriving at these interpretations is the question of whether the system keeps records that are required by a law or regulation. It is important to note that although there may be instances where systems need not comply with the requirements for electronic records any system used for GMP, GLP, or GCP activities must be validated. Not all systems will fall cleanly into one of the categories listed below. In these cases it is not possible to provide specific interpretation here and additional advice may be sought.

5.4.1 Document Management Systems

Document Management Systems accept electronic or scanned documents as input and facilitate management of them through various phases of their life cycle. These documents may be SOPs, reports, change control forms, regulatory submissions or any of a host of document types that must be maintained. Some systems have electronic signatures, while some use the hybrid approach, where a hand-written signature is used to authenticate a printout of an electronic document. Whether or not they use electronic signatures, Document Management Systems that hold regulated documents and are used for more than merely maintaining and reissuing paper reference versions must comply with the requirements for electronic records. If electronic signatures are used for regulated purposes they must also comply.

5.4.2 Real Time Systems (eg. PLCs)

These systems, typically used in manufacturing operations, generally collect data directly from equipment. The PLC itself does not need to comply with the electronic record requirements if there is no permanent storage of an electronic record in the device i.e. it is transient data. However, if the data is transmitted to another system such as SCADA or DCS, that system becomes a repository for the data, and, where the records are required by

Such systems are not actually maintaining regulated electronic records, and do not need to comply with the requirements for electronic record and electronic signatures. For example, in a system used for calibration tracking, the calibration schedule may be an electronic record, although in the low risk category, while the actual tracking messages that create alerts that the calibration is due, may not be. Of course, there must be adequate paper or electronic records to document the activities that are being tracked, such as actual training records or calibration records.

5.4.7 Material Management Systems

Material Management systems are used for a wide variety of functions. These systems are so diverse in design that it is impossible to make a generalisation that would always include or exclude them from needing to comply with ER/ES requirements. These systems need to comply when, as is usually the case, the records are stored and used for regulated purposes. Electronic signatures required by regulation must be in compliance.

5.4.8 Process Control Systems

Process control systems (for example SCADA and DCS) not only control process equipment, but also frequently capture data related to the process. These systems are often hybrid systems, and can include electronic signatures in some cases, where for example they form part of a batch record. Unless the system is used only to generate a print of data for inclusion in a regulated record, then, since these systems capture data from production, they may need to meet the requirements for electronic records where any of these are kept for regulatory purposes, and for electronic signatures if used and required by regulation.

5.4.9 Laboratory Information Management Systems (LIMS)

LIMS are frequently used by regulatory agencies as examples of electronic record systems, and are within the scope of the rule, both for electronic records, and for electronic signatures where used and required by regulation.

5.4.10 Laboratory Instruments/Equipment

Laboratory equipment must comply with ER/ES requirements if it stores records, which are subsequently used in electronic form for regulated purposes. Equipment that has the capability of storing such data electronically, especially if that data can be modified or deleted by an operator, is likely to need to comply. Some laboratory equipment only stores transient data and prints out the results directly or passes them to a supervisory system. As with any system, it is permissible to take a print of any record and make that the raw data provided it is verified as complete and accurate and the electronic version is not used for any further regulated purpose.

When equipment is connected to an information gathering or supervisory system, such as a LIMS, then the decision as to whether it is necessary for the equipment to comply with ER/ES requirements will be dependent upon its design. If the data (both raw and derived) is automatically uploaded to the LIMS and the data on the host system represents an accurate and complete copy of the record from the instrument, then the computer on the instrument can be considered to be storing only transient data and need not comply with ER/ES. In some cases, the LIMS or host system may not be able to upload an accurate and complete copy of the data, for example in a chromatography system, where a paper version may also not meet business needs. In that case, it may be necessary to store the chromatograms on the individual instrument that must comply with ER/ES.

