authorized by an individual to be the legally binding equivalent of the individual's hand-written signature.

3.6 Hand-written Signature Captured Electronically

A traditional hand-written signature entered into a computerised system using a stylus or other device.

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.

a paper copy but an electronic copy of the audit trail on a durable medium such as CD-R may be offered to the inspector to take away.

In this case the format of the data may vary, but it must be readable using readily available software such as Word, Acrobat, or Excel. The process for creating such an electronic copy should be documented.

5.2.4 Validation

All GXP regulated systems particularly those including electronic records and/or signatures must be validated according to their potential impact on patient safety, product quality or record integrity. Computer systems determined to have regulatory impact will be developed/acquired, validated, and maintained following a structured approach. The validation activities ensure accuracy, reliability, and consistent intended performance of the system.

5.2.5 Presentation and Copying of Records

Where electronic records are kept in place of paper, the ability to present the record in a human readable form is required with the content and meaning (data and metadata) of the original preserved. Ideally the system should have the ability to produce a printout that contains an accurate and complete representation of the original electronic record (including audit trail and metadata). Nonetheless it should be possible to generate an electronic copy in a common format (e.g. PDF, XML, SGML) and with the records content and meaning preserved for review by regulatory authorities. Basic manipulation of the copy i.e. search, sort or trend analysis should be possible with the copy where the original allows this.

5.2.6 Retention and Archiving

Just as paper records must be retained and archived for defined periods, electronic records, together with their metadata, should be available for the time period specified in the retention schedule for the specific record. In addition to the record itself, any associated audit trail information should be stored for the same time period, since the audit trail contains the details behind any changes that may have been made to the record.

It is also acceptable to transfer electronic records to paper or other traditional medium provided that the content and meaning (i.e. data and metadata) of the records are preserved. The decision on how to retain or archive records should consider the risks associated with the potential loss of the record and the changing value of the record over time.

Where a record is to be archived electronically there should be procedures in place for regular back-ups and refreshing/transferring of media as necessary. A regularly tested disaster recovery plan would be expected as added assurance that the data is protected over its lifetime.

There will be situations where computerised systems are replaced by newer ones, even if only hardware or software upgrades. When this occurs it is desirable for the data from the old system to be compatible with processing by the new system. If this is not feasible, then a properly documented and validated migration of data into the new system is acceptable if it can be shown that the new record is an accurate and complete copy of the original. Relevant available from the vendor and within the site to demonstrate the suitability of the device for its intended purpose.

Hand-written signatures may be captured electronically and executed to electronic records through the use of a stylus or similar device, in which case the image of the signature is saved 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 site's 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 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.

Some instruments interface with LIMS. For these instruments, the link to LIMS must be validated as well as the instrument itself, and the regulated records transferred from the instrument to LIMS must be considered electronic records within the context of the LIMS.

5.4.11 Interactive Voice Response Systems

Systems in this category not only capture data but also control clinical studies via telephone, typically using telephone keypad entries and voice commands. The data is then processed and stored within the system. The systems are often used to control stock and record patient data and statistics. These will be electronic records and may include electronic signatures.

5.4.12 Spreadsheets

Spreadsheets are used for a wide variety of purposes, from facilitating calculations in the laboratory to managing lists in a manner similar to a database. The use of the spreadsheet is the determining factor as to whether it needs to comply with ER/ES requirements.

If the spreadsheet is not modifiable by the user except to enter data and the final spreadsheet is printed and not stored for further regulatory purposes, then it should not need to be in compliance with ER/ES. However, for regulated uses, the spreadsheet must be validated and good change control practices in place. The use of a secure, validated document management system to manage spreadsheets is encouraged.

Where a spreadsheet is used as a database, such as for tracking training, calibration, or other GXP activities, then its need to comply with ER/ES requirements should be considered. If records are being stored for later use, then the ER/ES requirements for the spreadsheet are in principle no different from any other regulated application, with due consideration for the level of risk being taken into account.

5.4.13 E-mail

Any system used to transmit regulated electronic records is within the scope of ER/ES. The use of e-mail for transmission of regulated information is generally discouraged due to the difficulties in complying (for example, the need to validate). However if e-mail is used for this purpose, the business owner of the process using e-mail as a means of transmission must be aware of and own the accountability for the associated risk. Controls must be put in place to alleviate the risk and enable compliance.