1. Purpose

The purpose of this Guideline is to advise on the practices to be adopted when wishing or requested, to display or provide copies of electronic records to regulatory authorities, auditors and other similar third parties.

2. Scope and Applicability

This guideline applies to any data, document or other record held in any way in a computerized system, especially when used in the context of GxP, which is inspectable by or submitted to the FDA or other regulatory authorities. It is also recommended that this be applied to similar records being used in the context of financial or legal accountability.

3. Definitions

3.1 Electronic Record

Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved or distributed by a computer system.

3.3 Metadata

Data describing context, content and structure of electronic records and their management through time.

3.4 *Third Party*

For the purposes of this guideline, 'Third Party' refers mainly to regulatory authority inspectors, primarily from FDA. The principles defined may be applied to requests from other regulatory authorities and similar external organisations as appropriate.

4. Responsibilities

4.1 Central System Owner

- Have a full knowledge and understanding of the support responsibilities of a central system owner.
- Ensure that potential requests for information from the system are identified.
- Ensure that required functionality for record retrieval and copying is built into system design.
- Ensure that adequate training to retrieve and provide copies is provided to users/local implementation teams.

screen, care should be taken to avoid misunderstandings or misinterpretations of presented records as a result of incomplete or unclear definition or context. Operators/users of a system will be fully trained and therefore familiar with the terminology and meaning of fields etc on screens; it should not be assumed that the third party will be similarly familiar.

This is usually managed in paper-based inspections by a careful review of all records immediately before their presentation to ensure that the requisite knowledge is available to clarify any detail. This may not be possible when the third party is directly viewing a screen where a new record is presented 'at the touch of a button'. In this situation it is important that an individual spokesperson is appointed who has a full knowledge of the system as well as the business processes to which it relates. Where any doubts or anomalies arise then it is essential not to discuss them in the presence of the inspector but to clarify such issues internally and subsequently present a definitive statement to the inspector. The system should at all times be operated only by a trained user. In particular, normal security considerations must apply and special dispensations must not be given.

Requests by the inspector to operate the system personally must be declined by explaining that it is a controlled system with only trained and authorized users permitted to operate it.

Where practical it is permissible to offer a 'pre-production' or training version of the system as an alternative to give the inspector an understanding of the system.

5.3 Copying electronic records to paper

As the content of a record on paper is fully visible and can therefore be checked, this could be a preferred medium for passing records to an inspector.
This relies on the computer system from which the record is produced having been designed and validated to be able to demonstrate that the printed record is an accurate and (as far as practicable) complete (i.e. it includes metadata/ audit trail information) representation of the record. This can be onerous for a system with a wide range of available records.

A paper copy must be verified by the addition of an appropriate signature and date. A further identical copy must be kept for reference, as is normal inspection practice.

5.4 Electronic Copies of Electronic Records

5.4.1 General

The process for producing electronic copies must be part of the initial system design and implementation and must be verified during validation. Copies of valid data made via an unverified copying process should only be provided with a clear explanation of their status.

The capability of copying large volumes of records quickly should not detract from the need to consider carefully the content and format of the copied records to ensure that they are consistent with the request and the intended communication.

In particular, care should be taken when producing copies of records from a Computer

network, must be in compliance with the IS Security procedures and using previously validated routines.

5.5 Other Requirements

When a broad request for a copy is made by a regulatory inspector, clarification should be sought from the inspector as to whether all records from a system, file or field or a specified subset of records, is to be produced. In principle the copying of records should be restricted to the minimum acceptable subset.

Depending on the context it may be useful to describe to an inspector the process for generating electronic copies of records including the system and record validation procedures.

Security arrangements around access to electronic records and copies of them should be current good practices and not compromised by the act of copying.

5.5.1 Privacy considerations

5.5.1.1 Data protection (EU)

The EU data protection directive has introduced certain rules within Europe which apply to the *processing* of *personal data*. The term "processing" is widely defined to include obtaining, consulting, use, disclosure and recording of personal data. The term "personal data" means any information that is capable of identifying a living individual.

As the site may need to disclose personal data to regulatory authorities in order to comply with legal or regulatory requirements which apply to the business, the site will need to comply with the requirements of the directive as implemented into applicable national law (eg in the UK it is the Data Protection Act 1998).

In order to disclose personal data to regulatory authorities the site must comply with the following conditions:

(a) Where the personal data relate to patients (ie individuals that have taken part in a clinical trial), the site may only disclose their personal data if the patient has given his prior consent. (Note: consent should have been obtained at the time the patient agreed to take part in the clinical trial);

(b) Where the personal data relate to employees of the site, the site may disclose their personal data if the management believe that it is in legitimate interests to do so and the disclosure does not adversely affect the interests of the employee. The site must not disclose any information that relates to employees' health or medical condition.

(c) In all cases the site must ensure that individuals whose personal data are disclosed are made aware of the reasons for the disclosure. This is normally achieved by giving a "data protection notice" describing who the employees are, what they are going to do with personal data and any recipients of those data. Where the individual is a patient, the data protection notice will be built into the consent form and does not have to be given again. Where the individual is an employee, the data protection notice should be given at the time the employee joins the company or, if it is not given at that time, before the data are disclosed to the third party. Data protection notices can be sent by email,

