# 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

 

Access by Regulatory Authorities and Auditors to Electronic Records validation of the system must establish that this is part of its effective functionality.

#### *5.4.4 Copying Signature Information*

Where a record containing an electronic signature is to be copied, the system must be designed in such a way that the copy contains only the manifestation of the signature i.e. name, date and meaning, and not the input elements themselves, particularly where a password is used.

#### *5.4.5 Copy Medium*

Electronic copies will typically be provided on floppy disk or CD ROM. Consideration should be given to the security of records released in this way and appropriate confidentiality agreements secured in advance with the recipient of the electronic copies. If there is any likelihood of the record being released into an 'open' network or system then encryption or other suitable means to protect the record should be employed. Particular care should be exercised if the copy record is to be transmitted electronically to an external recipient, as this will almost certainly involve the use of an open system such as the Internet. Any direct download to a third-party-owned PC, i.e. connection to the site 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).

 