UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE: Electronic Data Quality Policy for Clinical Research	REFERENCE: Reformat
CATEGORY: Information Technology	PAGE: 1
	SUPERSEDES: POL-UMIT-EDQ-001-03
APPROVER: David Ertel Interim Senior Vice President Business and Finance	VERSION: 2 EFFECTIVE: May 16, 2017

I. PURPOSE:

It is a key part of the overall mission of the University of Miami (UM) to serve patients and society by maximizing the value of its biomedical research to advance the quality of clinical trial data and the effectiveness of patient care.

Similarly, it is UM's mission to provide state-of-the-art clinical trial and electronic data of the highest integrity to advance the science and practice of electronic data management in all UM research studies and improve patient and subject care.

These services are subject to the regulations and guidance of many governing bodies. Accordingly, UM senior leadership will provide clinical research, trial management and study data processing services to:

- Support the scientific objectives of UM initiatives by leveraging core competencies in computer based technologies.
- Comply with electronic records, electronic signatures and data privacy regulations in effect when it delivers electronic data services.
- Provide data handling services to assure that regulated electronic data are attributable, legible, contemporaneous, original and accurate (ALCOA).

When using electronic trial data handling and/or remote electronic trial data systems, UM shall:

(a) Ensure and document that the electronic data processing system(s) conforms to the established requirements for completeness, accuracy, reliability and consistent intended performance (i.e. validation).

(b) Maintain SOPs for using these systems.

(c) Ensure that the regulation sensitive systems are designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e. maintain an audit, data and edit trail).

(d) Maintain a security system that prevents unauthorized access to the data.

(e) Maintain a list of the individuals who are authorized to make data changes.

(f) Maintain adequate backup of the data.

(g) Safeguard blinding, if any (e.g. maintain blinding during data entry and processing).

This document provides the basic policy for implementing a regulation sensitive infrastructure and application framework that complies with various applicable regulations and assures data quality at UM.

II. <u>SCOPE:</u>

Management recognizes its responsibility and is committed to developing and delivering clinical trial services and general business practices at UM in an ethical manner consistent with the principles outlined below.

The basic principles outlined in this document will be applied to computer systems, electronic equipment and infrastructure to establish technological requirements, such as audit trails, electronic signature components, timestamps and timeouts.

Procedural requirements, including identification of responsibilities, training and responsibilities associated with electronic signatures, back-ups, disaster recovery plans, validation, security and identification checks, will be specified in Standard Operating Procedure (SOP) and Standard Working Procedure (SWP) documents.

III. <u>POLICY:</u>

<u>Basic Principles and Guidelines:</u>

Below are the basic principles for achieving compliance with FDA 21 CFR Part 11:

Basic Principle 1 –

UM shall take the necessary actions to ensure the proper implementation of procedures and technologies to achieve compliance with various regulatory requirements, such as safeguarding patient health information, electronic records and signatures.

Basic Principle 2 –

Computer systems and electronic equipment shall be evaluated for applicability and where necessary, compliance with regulatory requirements.

Basic Principle 3 –

Based on the results obtained from the evaluation in Basic Principle 2, remediation plans should be prepared and implemented to correct deficiencies. Progress of remediation plans should be monitored.

Basic Principle 4 –

New computer systems and electronic equipment to be implemented must be evaluated for compliance with Part 11. These may not be implemented until compliant with Part 11 requirements. However, in cases where no available technical solutions fully comply with regulations' technical requirements, procedural controls and solutions should be implemented to ensure compliance.

Basic Principle 5 –

New systems must be assessed prior to introduction to determine whether they meet applicable regulatory requirements pertaining to their intended use at UM. To aid in this assessment, it is recommended that end-user requirement specifications be prepared for relevant compliance with Part 11 and discussed with the supplier. Any deficiencies should be discussed with the service provider and where technically feasible, corrected or addressed prior to introduction.

Basic Principle 6 –

In addition to electronic records of computer systems and electronic equipment currently in service, electronic records of retired computer systems and other electronic equipment subject to regulatory requirements, such as hand-held devices and laboratory equipment which store data, need to be managed.

Basic Principle 7 –

Computer systems and electronic equipment subject to regulatory compliance must be validated in accordance with corporate validation standards and policies, and the validation must include a solution that assures regulatory compliance.

IV. DEFINITIONS:

N/A

V. PROCEDURE:

N/A