



PQE

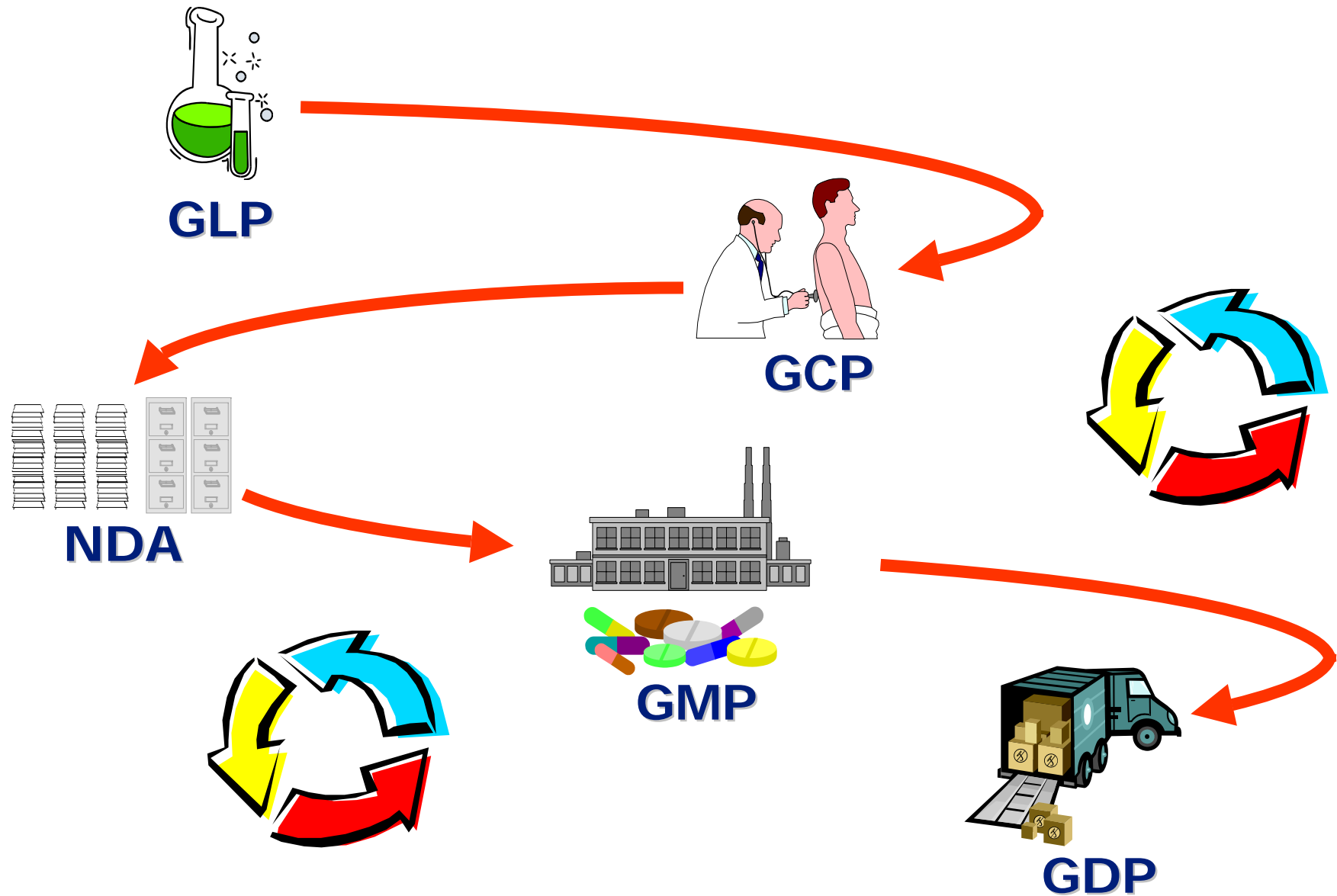
Pharma Quality Europe s.r.l.

Audit to Computerized Systems

GIQAR

Danilo Neri
Roma , Novembre 2006

Regulatory Requirement to maintain the Chain of Evidence



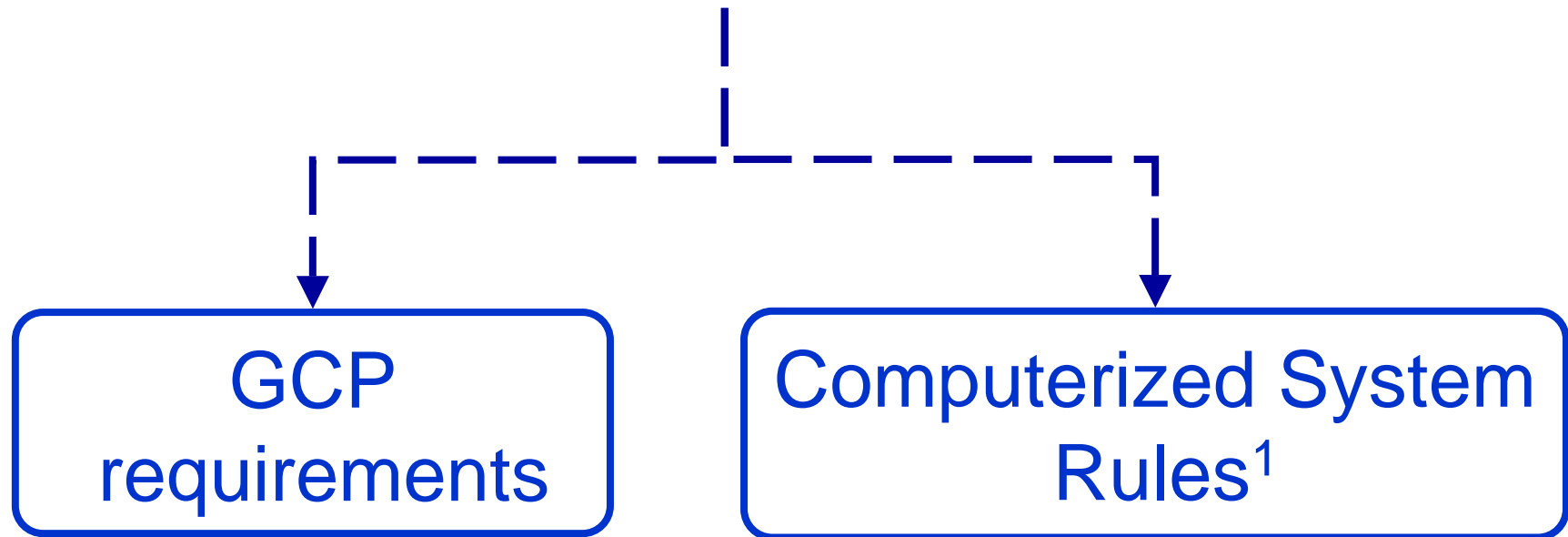
Computer Systems used in Clinical Study

- Randomization system
- Data Capture System
 - automatic measuring device
 - manual data input (In house data entry, Remote Data Entry)
 - automatic data input
- Clinical Database Management System
- Drug Supplies Accountability System
- Statistical System
- Drug Safety System



Clinical Systems

have to comply with



¹ for CS used in
a regulated environment

Computerized System Rules

FDA - 21 CFR Part 11: Electronic Records; Electronic Signatures. August 1997

FDA – 21 CFR Part 21: Protection of Privacy

The Rules governing Medicinal Products in the EU, Volume IV, 1998, Annex 11: Computerised Systems

Directive 1999/93/EC: Community framework for electronic signature

Directive 95/46/EC: Data Protection

Directive 2002/58 of the European Parliament and of the council of 12 July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

DPR n. 318, Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2 della legge 31 dicembre 1996, 28 luglio 1999

DL 30/06/2003, n° 196 codice in materia di Protezione di dati personali



Computerized System Guidelines

By Regulatory Authorities

- ✓ **US FDA - Guide to Inspection** of Computerized Systems in Drug Processing – 1983
- ✓ **US FDA - General Principles of Software Validation**; Final Guidance for Industry and FDA Staff, January 2002
- ✓ **US FDA - Guidance for Industry: 21 CFR Part 11: Electronic Records and Electronic Signatures: Scope and Application, Final August 2003**
- ✓ **US FDA - Guidance for Industry: Computerized Systems used in clinical trials** (final version April 1999)
- ✓ **US FDA - Guidance for Industry: Computerized Systems used in clinical trials** (revision 1 draft September 2004)



Computerized System Guidelines

By Organizations

- ✓ **ACDM/PSI: Computer Systems Validation in Clinical Research** - A practical guide” ACDM/PSI, 1998
- ✓ **GAMP Forum, Good Automated Manufacturing Practice** - Supplier Guide for Validation of Automated Systems in Pharmaceutical Manufacture, v. 4.0 December 2001.
- ✓ **PIC/S Good Practices for computerised systems in regulated “GxP” environment**, Pharmaceutical Inspection Co-operation Scheme final guidance, rev.2 - July 2004



The fundamental guidances

Guidance for Industry Computerized Systems Used in Clinical Trials

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Comments and suggestions regarding this draft document should be submitted within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5650 Fishers Lane, rm. 1061, Rockville, MD 20852. All comments should be identified with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this draft document contact Patricia M. Beers Block 301-627-3340.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)

September 2004
Compliance

Revision 1

Code of Federal Regulations

21 CFR Part 11; Electronic Records; Electronic Signature



August, 1997



PHARMACEUTICAL INSPECTION CONVENTION
PHARMACEUTICAL INSPECTION CO-OPERATION SCHEME

PI 011-2
1 July 2004

PIC/S GUIDANCE

GOOD PRACTICES FOR COMPUTERISED SYSTEMS IN REGULATED "GXP" ENVIRONMENTS

© PIC/S July 2004.
Reproduction permitted for commercial purposes,
provided that the source is acknowledged.

Editor: PIC/S Secretariat
P.O. Box 6999
CH-1211 Geneva 11
email: office@picScheme.org
web site: <http://www.picScheme.org>

1 July 2004

PI 011-2

The fundamental Responsibility

“Although much of the software validation may be accomplished by outside firms ... software vendors, the ultimate responsibility for program suitability rests with the pharmaceutical manufacturer. Records of software validation should be maintained by the drug establishment.”

.

PIC/S Guidance: Good Practices for Computerized Systems in Regulated GxP Environment



Quality and Integrity

DATA SHOULD BE

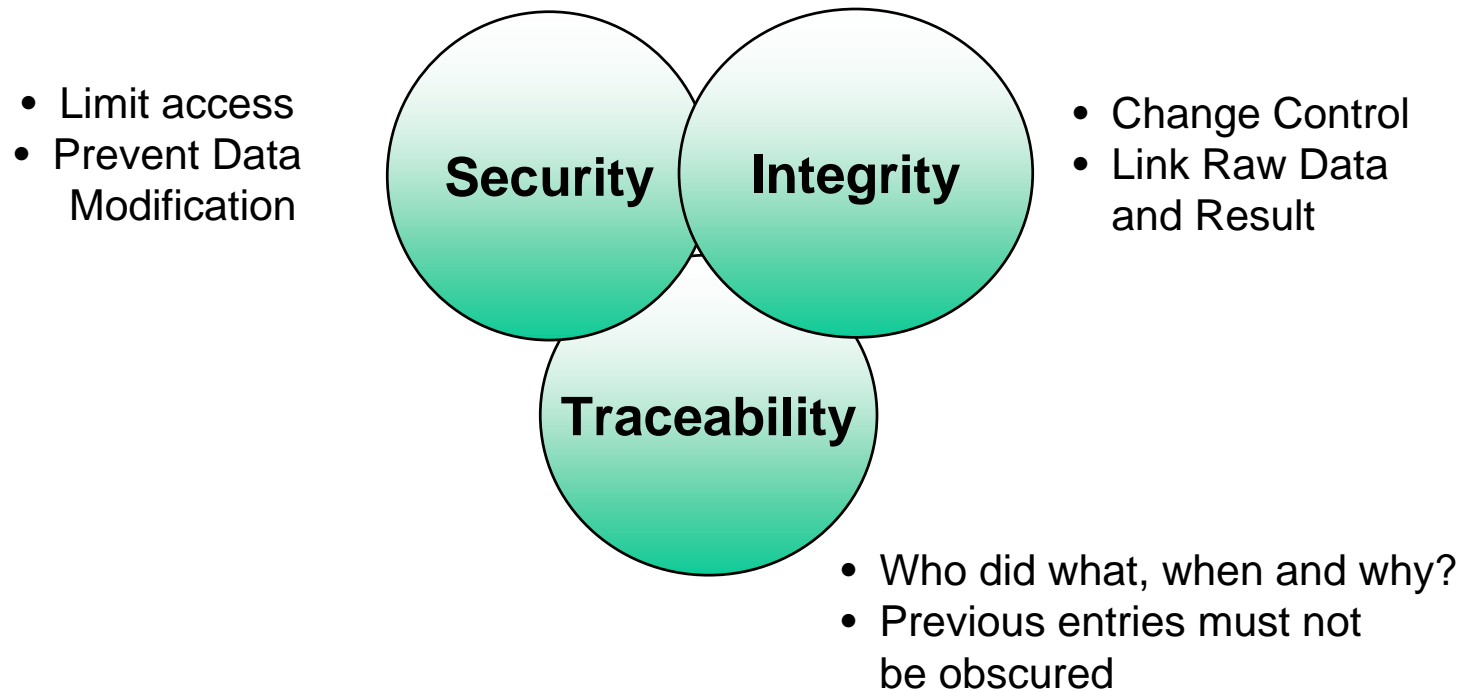
- ✓ **attributable,**
- ✓ **legible,**
- ✓ **contemporaneous (timeliness),**
- ✓ **original**
- ✓ **accurate**

regardless the format

Paper format = electronic format



Regulatory Implication on Electronic Data



Trustworthiness of electronic records is ensured by appropriate measures for data security, data integrity and traceability

Computerized Systems used in clinical trials

I.	INTRODUCTION.....	2
II.	BACKGROUND	3
III.	GENERAL PRINCIPLES	4
IV.	OVERALL APPROACH TO MEETING PART 11 REQUIREMENTS	5
V.	STANDARD OPERATING PROCEDURES.....	5
VI.	DATA ENTRY	5
A.	Computer Access Controls.....	5
B.	Audit Trails or other Security Measures	6
C.	Date/Time Stamps.....	7
VII.	SYSTEM FEATURES.....	8
A.	Systems Used for Direct Entry of Data	8
B.	Retrieval of Data and Record Retention.....	8
VIII.	SYSTEM SECURITY	8
IX.	SYSTEM DEPENDABILITY.....	9
A.	Legacy Systems	10
B.	Off-the-Shelf Software.....	10
C.	Change Control.....	11
X.	SYSTEM CONTROLS.....	12
XI.	TRAINING OF PERSONNEL	12
XII.	COPIES OF RECORDS AND RECORD INSPECTION.....	13
XIII.	CERTIFICATION OF ELECTRONIC SIGNATURES	13
	DEFINITIONS	15



Part 11 vs ICH E6 Requirements 1/2

Requirement	Part 11	ICH E6
Validation of Computer system	11.10.(a)	5.5.3.a
Accurate and Complete Copies of Record	11.10.(b)	4.9.7
Data Protection	11.10.(c)	2.10; 4.9.1; 5.5.3.f
Limiting Access	11.10.(d)	§ 2.11; 5.5.3.d
Audit Trail	11.10.(e)	4.9.3; 5.5.3.c



How to Audit a Computer System?



PIC/S Audit Agenda

Table 4
Annex 11 – Inspector's Checklist

Point	Requirement	Inspector's Check/Comment
Personnel (1)	Key personnel/computer specialists co-operate.	
Personnel (1)	Project and user personnel are trained and any necessary experts are involved.	
Validation (2)	Life-cycle model; formal policy and procedures in place.	
System (3)	Influence of environment	
(4)	There is a written, up to date, detailed description of the system.	
(5)	Software has been produced according to a quality assured system.	
(6)	Checks of data and calculations built in.	
(7)	System tested and validated. Verified against previous/or manual system being replaced.	

PIC/S Audit Agenda

Table 4
Annex 11 – Inspector's Checklist

(8)	Data entry and change only by authorised personnel. Password / security management.	
(9)	Critical data (GXP data) verified by a 2 ^o person, or by a validated electronic method.	
(10)	Audit trail for data entry and processing.	
(11)	Alterations to system and programs subjected to rigorous change controls, including re-validation and approvals.	
(12)	Printed copies of electronically stored data available if needed?	
(13) and GMP 4.9	Physical and logical protection of data. Information security management and change management.	
(14)	Data back up procedures; separate and secure media and locations.	
(15)	Alternative routine arrangements established in the event of system failure.	

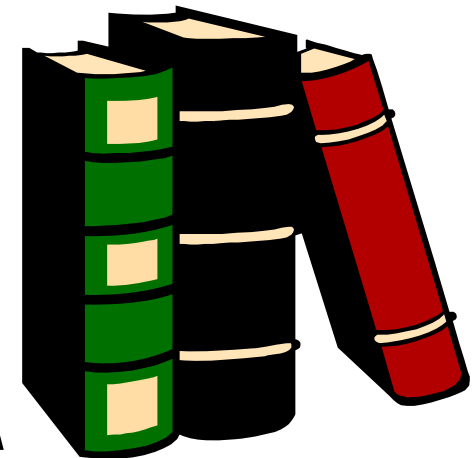
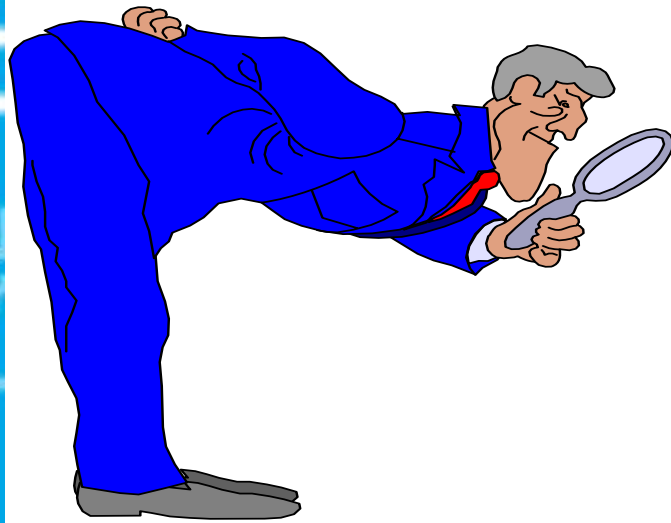
PIC/S Audit Agenda

Table 4
Annex 11 – Inspector's Checklist

(16)	Validated alternative arrangements (15) defined and documented. Records of failures and remediation exist.	
(17)	Records show the analysis of errors and corrective actions taken.	
(18)	Service level agreements or contracts in place for services provided by outside agencies for computerised systems at regulated user's sites.	
(19)	Responsibilities in chain of release of batches defined and linked to QP.	

Audit tools

- Personnel Interviews
- Documents Assessment



Audit preview

- What the system is supposed to do
- Which process/es is/are supported by the system
- Who is responsible for the system use
- Who is responsible for the system validation status
- Level of integration with other company system



Validation Documentation

- **User Requirements**
- **Validation Plan**
- **Test Protocols**
- **Test Results & Report**
- **Validation Report**
- **Traceability Matrix**



System Documentation

- **User Manual**
- **SOPs**
 - Security
 - Back up
 - Disaster Recovery
 - Change control
 - Maintenance
 - Periodic Review
 - Training

System Security

- **Control the access to the system**
 - Physical access
 - Logical access
 - Computer room
 - Client(s)
- **System User**
 - Training records



System Security

- **Back up Procedure**
 - Frequency of the Back up
 - Media archiving
 - Check the log of the back up execution
- **Disaster Recovery**
 - Test result



System Maintenance

- **Change control SOP**
 - Change Log
 - Have under control changes on Data, not only on Applications
- **Maintenance SOP**
 - Errors Log

Some useful questions

- Who is responsible for the system
- Who is the system Administrator
- How many users
- What are the profiles of the users
- Who manages the user's profiles
- What is the expiry time of the password
- What happens when a users loss his/her password
- What about user's training

Some useful questions

- Which SW version is installed and used
- What kind of maintenance is performed on the system and by who
- Who has the responsibility for evaluating the impact of system changes
- How many system errors occur in the last three months
- Have you tested the system recovery
- Are you used to perform the recovery test periodically

Some useful Checks

- Cross-check between the user listed in the system and the **User's List** (generally attached to the Access Control SOP)
- Cross-check between the **software version** installed and used and the software version recorded in the relevant IQ document
- Check the last **back up** registration
- Check whether the “**proposed actions**” generally include in the Validation Report have been implemented

Auditing a CRO

The purpose of the audit is to assess compliance by the CRO with internationally recognized good clinical practice regulations



Auditing a CRO

The Audit will focus primarily on the activities carried out in relation to the conduct of clinical trials, with particular emphasis on the following:

- General Documentation
- Study Management
- SOPs approval flow
- **Data Management and Documentation Control (Paper & Electronic)**
- **Computer System**
- Handling of Investigational Products
- Monitoring activities
- Quality Assurance activities
- Handling of Adverse Events
- Archive Facilities

Electronic Data Management

- Flow of data and information to and from Investigator Sites
- Flow of data recorded on CRFs
- Review of CRFs
- Audit Trail
- Management of Queries
- Quality Control Activities
- Closure of Database



Computer System

- **Inventory of Hardware and Software**
- **Access procedures**
- **Software Documentation**
- **Validation documentation**



Auditing a GCP System

The purpose of the audit is to assess compliance by the company' computerized systems with internationally recognized good clinical practice regulations

GCP Systems Audit Agenda

APPLICATION

Requirement Specifications

Validation Master Plan

Risk Analysis (bespoke code Vs off the shelf package, ...)

Validation Protocol

SYSTEM CONFIGURATION

Hardware/Software Lay-Out

Hardware requirements

Historical Log



GCP Systems Audit Agenda

SOFTWARE DEVELOPMENT

Functional Specifications

Design Specifications (Methodology, Flow-diagrams, List of programs, ...)

Source Code

TESTING

Functional (OQ) Testing (Test data, Test Results, ...)

Integrated Process Testing (PQ) (Stress testing, worst cases, critical decision paths...)



GCP Systems Audit Agenda

USER DOCUMENTATION

Manuals

Technical Instruction

OPERATING PROCEDURES

Configuration Management (Version Control, Source Control,)

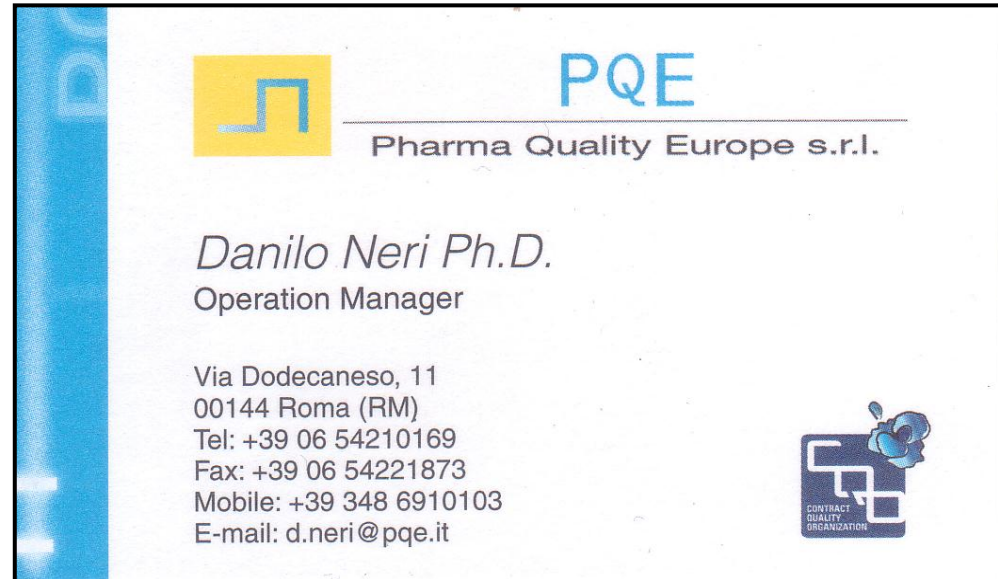
Change Control (Bug Tracking, System Problem Reporting, ...)

Maintenance

Security (Back Ups, Disaster Recovery. Contingency Plan)

Training

Thanks for your attention



*Should you have any question,
feel free to contact me*

