Training Course
Computerized System Validation in the Pharmaceutical Industry
Istanbul, 16-17 January 2003

# Electronic Records and Electronic Signatures (21 CFR Part 11)

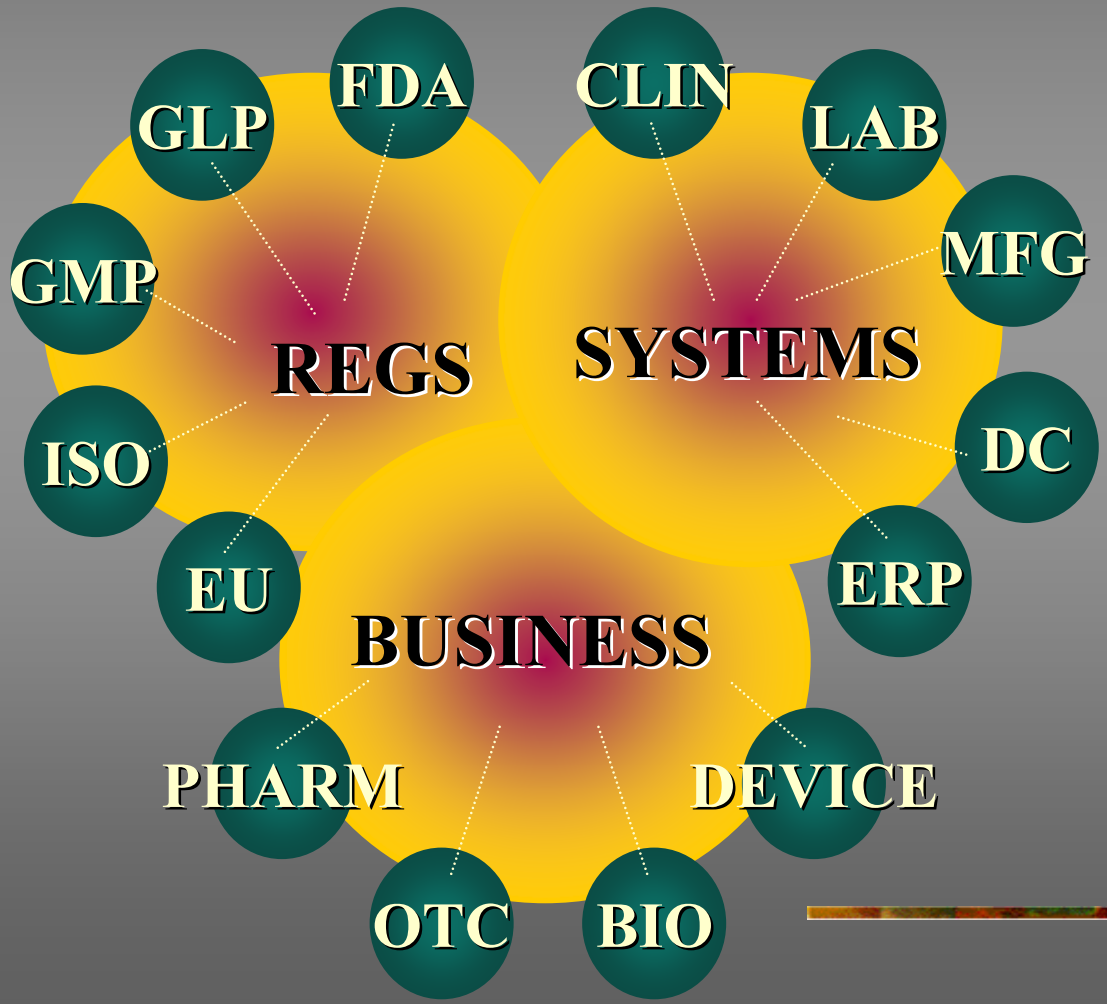
Hans-Beat Jenny, SwissMedic, Basel

Wolfgang Schumacher, Roche Pharmaceuticals, Basel

# Agenda

- Introduction to 21 CFR Part 11
- Definitions
- How to proceed to be in compliance?
- The new Validation Guidance (Draft August 2001)
- The new Maintenance Guidance (Draft July 2002)
- The new GERM documents (Parts 1,2,3)
- What can QA do to reduce Part 11 confusion?
- New trends

# Multiple Landscapes



# Part 11 Overview

- Substantive rule from 20 August 1997
- Applies to any e-record in any FDA regulated work including legacy systems
- Criteria for e-records and e-sigs:
  - Trustworthy and reliable
- E-sigs equal meaning to hand-written signatures
- Objective: prevention of fraud

# What is 21CFR11?

- 21CFR = FDA, Code of Federal Regulations
- 21CFR58 = GLP
- 21CFR210 = GMP, Drugs (General)
- 21CFR211 = GMP, Drugs (Finished Pharmaceuticals)
- 21CFR312 = Inv. New drug Application (GCP)
- 21CFR314 = FDA Approval of new drug (GCP)
- 21CFR6xx = GMP, biologics
- 21CFR820 = GMP, Devices
- ……..
- ***21CFR11 = Electronic Records; Electronic Signatures***

# 21 CFR Part 11, Basics

Electronic records equivalent with paper records

- Storage, retrieval and copying in full retention period
- Submitting to FDA

Protection of electronic records

- Security (physical and logical)
- Validation
- Audit trail

Permission to use of electronic signature

- Equivalent with handwritten signatures
- Name, date and meaning
- Linking of signature to record

# Compliance Policy Guide CPG 7153.17

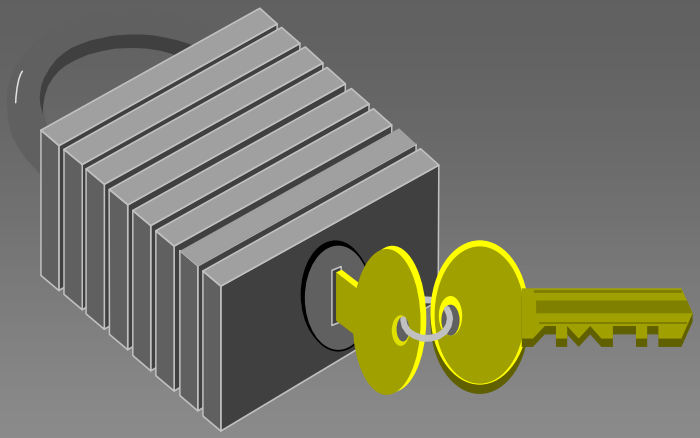
**Acknowledging 'not all older systems fully compliant by Aug 20, 1997'**

- 'firms must take steps to achieve full compliance'
- 'Regulatory actions based on case by case evaluation'
- 'FDA auditors should intensify their scrutiny of e-recs'

**Calls for firms to**

- have a 'reasonable timetable'
- 'promptly modify' any system not in compliance
- 'be able to demonstrate progress'
- 'have procedural controls in place by now'

# Definitions



*Closed System 11.3(4) :* "Closed system means an environment in which system access is controlled by persons who are responsible for the content of the electronic records that are on the system"

*Person:* "Person includes an individual, partnership, corporation, association, government agency, or organizational unit thereof, and any other legal entity."

# Rawdata - Processed - Meta Data

| Rawdata | Meta data | Processed data |
| --- | --- | --- |
| Signal (mV)<br>peak slices | processing parameters<br>- integration parameters<br>- calibration tables | peak area<br>amount |

# Workflow of Laboratory Applications

| Instrument | PC | Server/Database |
| --- | --- | --- |
| measurements | data acquisition<br>data evaluation | data management<br>archiving |

# Part 11 - Data Integrity

## Key elements for compliant systems

- Ability of FDA to inspect data
- Prevention of fraud
- Ability to retain data for the required time interval

# Archiving

*11.10 (c): Procedures and controls shall include: Protection of records to enable their accurate and ready retrieval throughout the records retention time.*

- Definition of retention period
- Selection of storage media
- Migration of data to new systems

Many issues covered in the recent FDA ERES "Maintenance of Electronic Records" Guidance (Issued for comments: Sept. 2002)

# The Steps of Part 11 Implementation

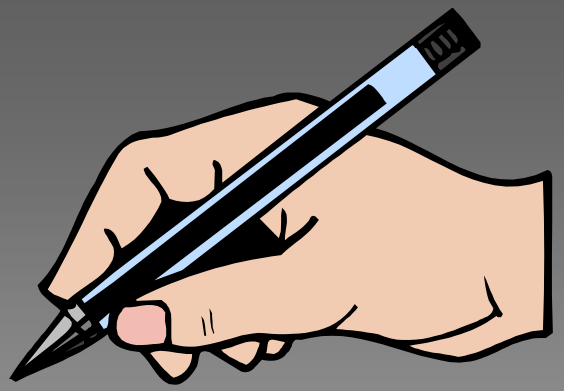
- Establish an assessment team, knowledgeable in Part 11
- Prepare a list of all computerized systems
- Evaluate which systems involve FDA-regulated electronic records and/or electronic signatures
- Assess the state of compliance (gap analysis)
- Assess the risk
- Define the action plan
- Set-up administrative/procedural controls
- Train people

# Definitions

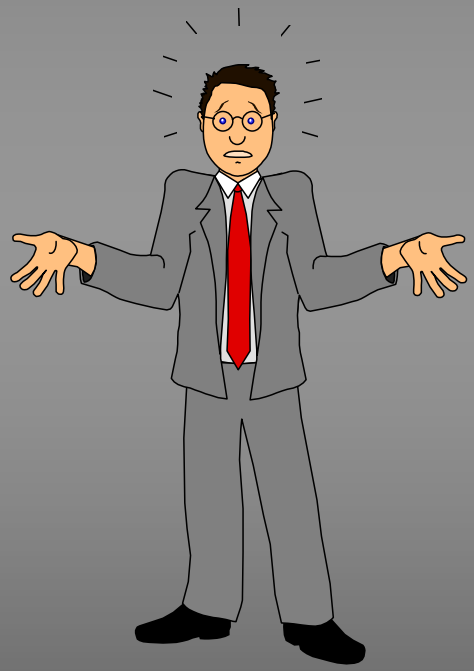
*Handwritten Signature:*

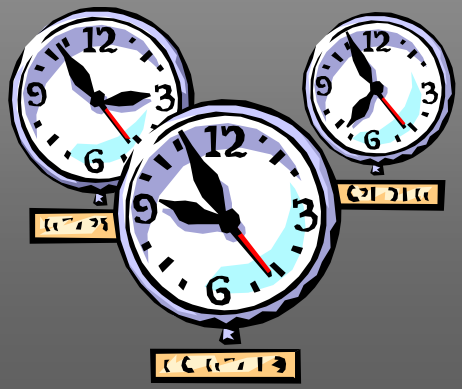
Scripted name or legal mark of an individual handwritten by that individual and executed or adapted with the intention to authenticate a writing in permanent form

# Legal Signature



- A legal signature is the mark
  - of a specific **individual**
  - against a specific **document**
  - at a specific **time**
  - given with specific **intent**





# Electronic Signature Types

## Biometric (Sec. 11.3 Definitions)

- Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

**Eye Recognition** | **Finger Print** | **Voice Recognition** | **Signature**

# ISPE/GAMP & PDA Cooperative Effort
# New Part 11 Interpretations

## Good Practice and Compliance for Electronic Records

- Part 1: **G**ood **E**lectronic **R**ecords **M**anagement (GERM) Practices
- Part 2: Complying with 21 CFR Part 11, Electronic Records and Electronic Signatures
- Part 3: Models for Systems Implementation and Evolution

# GERM Part 1

## *Operations & Infrastructure*

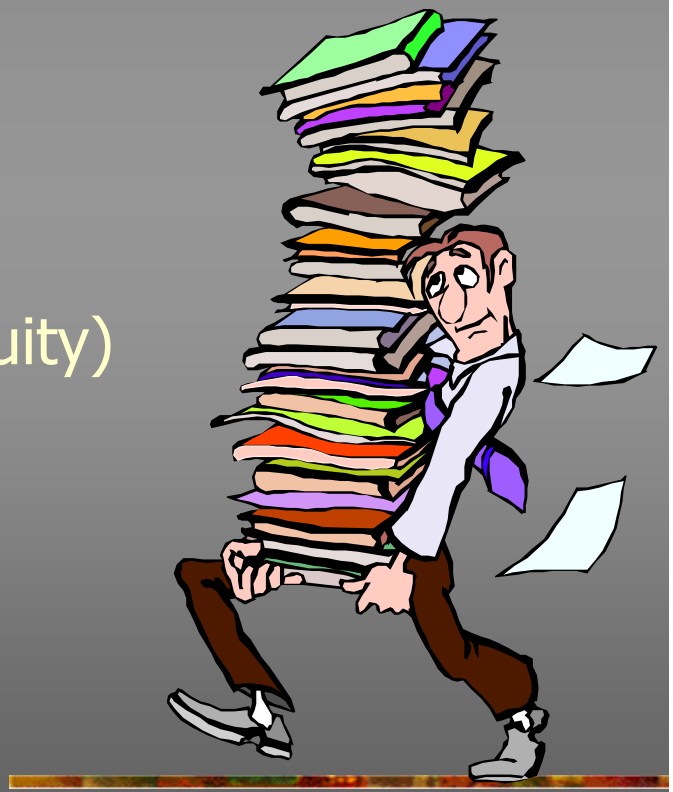
Contents

- Computer Operations
- Data Center Functions
- Workstations / Desktops / Laptops
- System Documentation
- Physical Protection of Records
- Logical Security
- Identification / Authentication and Record Integrity and Confidentiality
- Networks
- Configuration Management
- Database Integrity
- Business Continuity / Disaster Recovery

# GERM Part 1
## *Records Retention*

Contents

- Which Records to Retain?
- Media and Storage Conditions
- Retrieval
- Long Term Access (Knowledge Continuity)
- Digital Signature Migration
- Retention of Original System
- Record Deletion



# GERM

Good Practice and Compliance for Electronic Records and Signatures

**Part 2**

Complying with 21 CFR Part 11,Electronic Records and Electronic Signatures

- Very big document (Draft approx. 90 pages)
- Draft tested, industry submitted input; going through final peer review; in final stages of preparation for publication, to be published very soon
- Focus is towards the system designers of electronic record and electronic signature environments

# Electronic Records; Electronic Signatures Validation Guidance

## Key Elements of Computer System Validation

- System Requirements Specifications
- Installation Qualification
- Dynamic Testing
- Static Verification Techniques
- Independence of Review
- Change Control

# Electronic Records; Electronic Signatures Validation Guidance

Extent of validation is determined by:

- System Risk
- System Complexity

# 5. Key Principles
## 5.1. System Requirements Specifications I

"Without establishing user needs and intended uses, we believe it is virtually impossible to confirm that the system can consistently meet them."

- Evidence of correct implementation in the system,
- Traceability to
  - system design requirements
  - specifications.

# 5. Key Principles
# 5.1. System Requirements Specifications II

Part 11 specific requirements

- Record authenticity, integrity, signer non-repudiation and confidentiality, if appropriate (11.10, closed systems).
- Similar requirements for open systems (11.30), e.g.
  - digital signatures,
  - encryption.

# 5. Key Principles
## 5.1. System Requirements Specifications III

Requirements not addressed specifically in Part 11 are to be considered,

- trustworthiness and
- integrity

  of electronic records,
- system performance, e.g.
  - Scanning processes
  - Scalability
  - Operating environment of the system.

# Electronic Records; Electronic Signatures Validation Guidance

## Complete Testing

- Structural testing [white-box testing]
- Functional testing [black-box testing]
- Program build testing

# Electronic Records; Electronic Signatures Validation Guidance

## Key Testing Considerations

- Simulation testing
- User site testing
- Test results suitable for independent review

# 5.2.2. Validation Procedures

should include:

- Detailed steps of validation activities,
- description of
  - computer system configuration
  - test methods with
    - expected results
    - objective acceptance criteria.
- Review and approval by management

# 5.3. Equipment Installation

(Installation Qualification)

- Hardware & Software properly installed
- Adjustments and calibrations performed.

- User Manuals
- SOPs
- Equipment lists
- Specifications

should be available for reference

# 5.5. Static Verification Techniques

Numerous verification steps include

- Static analyses, e.g.
  - document inspections,
  - code inspections,
  - walk-throughs,
  - technical reviews.

They help to reduce the amount of system level functional testing.

# 5.6. Extent of Validation

Factors to consider for the determination of the appropriate extent of validation:

- Risk for the product concerning its
  - quality
  - safety
  - efficacy.
- Risk for data integrity, authenticity, and confidentiality.
- System's complexity.

# 6.1. Commercial, Off-The-Shelf Software I

- Need for validation,
  "just as programs written by the end users".
- Marketing alone is "no sufficient proof" of programs performance suitability.
- Efforts are different as
  - source code and
  - development documentation

  are not available for the users

# 6.1. Commercial, Off-The-Shelf Software II

Validation is required for

- program macros and
- customization.

# 6.1. Commercial, Off-The-Shelf Software III

## 6.1.1. End User Requirements Specifications

Validation is required for

- program macros and
- customization.

# 6.1. Commercial, Off-The-Shelf Software IV

## 6.1.2. Software Structural Integrity

If source code is not available for inspection:

- Identification of known program limitations.
- Evaluation other end user experience.
- Identification of known software problems and their resolutions.
- Reliable audit of the software developer by
  - user organization or
  - trusted and competent third party.

# Part 11 - What could be done first line?

Restrict access to critical areas, e.g.

- Limit system administrator rights to the necessary number of individuals
- Restrict the access to data
- Prevent the deletion of data by users
- Install audit trail functionality

# Immediate activities

- Implement solutions that rapidly increase overall state of compliance: Procedural solutions
- Implement controls (temporary procedures or add-ons) to reduce data integrity risk

# Future activities

Implement technical solutions

- Contact suppliers
- Get budget
- Allocate resources

# FDA Inspection Practices

- No inspections solely to check compliance with 21 CFR Part 11
- Compliance is evaluated during routine or pre-approval inspections
- Most probably the inspector will check Part 11 compliance when looking at records

# New Trends ?!

# The Pink Sheets, October 21, 2002

Manufacturing Controls Seminar in Parsippany, NJ Oct. 10-11.

According to CDER director Dr. Janet Woodcock, FDA intends to issue a policy statement on how its risk-based good manufacturing practices initiative will affect 21 CFR Part 11, its electronic records and electronic signatures regulation, by early next year. Before a policy statement is released, Dr. Woodcock explained, FDA needs "to reach some agreement generally about what risks we are trying to avoid and what risk is in the context of electronic records."

# The Pink Sheets, October 21, 2002

Manufacturing Controls Seminar in Parsippany, NJ Oct. 10-11.

New Jersey District Director Douglas Ellsworth told the meeting that the majority of recent FDA consent decrees have been due to poor oversight by senior company management, not problems inherent in firms' manufacturing controls.

# The Pink Sheets, October 21, 2002

Manufacturing Controls Seminar in Parsippany, NJ Oct. 10-11.

"Woodcock noted that there will be a complete reevaluation of the regulation [21 CFR Part11].

There are a number of unintended consequences of the regulation that FDA is observing. The fact that there are no final guidances is problematic for both industry and the FDA. Current interpretation may have blocked technical improvements. She indicated that it is wrong to ask for continued investments from industry if there is no firm guidance on the requirements."