



21 CFR Part 11

Preface

From the beginnings of civilization people have been concerned about the quality and safety of foods and medicines.

Regulation of food in the United States dates from early colonial times. Federal controls over the drug supply began with inspection of imported drugs in 1848.

How it all Began

- **1906** The original Food and Drugs Act is passed on June 30 and Meat Inspection Act is passed the same day .
- **1927** The Bureau of Chemistry is split into two departments:
 1. The Food Drug & Insecticide Administration
 2. Bureau of Chemistry and Soils
- **1937** ELIXIR OF SULFANILIMIDE containing diethylene glycol, a poisonous solvent kills 107 many of which are children.
- **1938** THE FEDERAL FOOD, DRUG, AND COSMETIC (FDC) ACT is passed by Congress.

Milestones

- **1940** The FDA is transferred to the Federal Security Agency.
- **1944** PUBLIC HEALTH SERVICE ACT is passed, covering a broad spectrum of health concerns, including regulation of biological products and control of communicable diseases.
- **1949.** FDA published the **first**

GUIDANCE TO INDUSTRY

This guidance “Procedures for the Appraisal of the Toxicity of Chemicals in Food,” came to be known as the “black book.”

Milestones

- **1962** THALIDOMIDE, a new sleeping pill, is found to have caused birth defects in thousands of babies born in western Europe, which lead to public support for stronger drug regulation.
- **1976** MEDICAL DEVICE AMENDMENTS passed to ensure safety and effectiveness of medical devices, including diagnostic products. The amendments require manufacturers to register with FDA and follow quality control procedures. Some products must have pre-market approval by FDA; others must meet performance standards before marketing
- **1988** Food & Drug Administration Act officially establishes FDA .

Part 11 Origins to Present

- 1994 : Proposed Rule
- 1994: 1997 Industry responses
- 1997: 21 CFR Part 11, Electronic Records; Electronic Signatures, was originally issued in 1997. Its proposed to: “Provide criteria for acceptance by the FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper.”
- 2001-2002: Guidance documents
- 2003: New scope and new guidance
- 2007: New Part 11

1997 to 2003: What Changed?

- Responsibility for Part 11 moved from the Office of Regulatory Affairs (ORA) to the Center for Drug Evaluation and Research (CDER)
- Part 11 rule may be revised
- New draft guidance replaced old draft guidance
- Enforcement policy withdrawn
- Reinforcement of predicate rule requirements
- Promotion of risk-based approach
- Narrowed interpretation of Electronic Record
- Enforcement discretion for legacy systems (pre 1997)

What didn't Change

- No changes to Electronic Signatures
- No changes to Electronic Record Clauses related to
 - System access controls
 - Enforce sequence steps
 - Application access controls
 - Device checks
 - Competence of people
 - Document controls
- No changes to open systems
- No changes to signature and record linking

21 CFR Part 11 Guidance

Guidance for Industry Computerized Systems Used in Clinical Investigations

U.S. Department of Health and Human Services
Food and Drug Administration (FDA)
Office of the Commissioner (OC)
May 2007

- Supersedes all old Guidance Documents
- Contains detailed Recommendations on
 - Study Protocol
 - SOPs
 - Source Documents and Retention
 - Internal and External Security Safeguards
 - System Features such as
 - Data Entry and Retrieval
 - Systems Documentation
 - Systems Controls
 - Change Control
 - Training of Personnel

21 CFR Part 11 - Overview

- Part 11 contains detailed guidelines on how to manage electronic records and electronic signatures in order to maintain accuracy and security
- Part 11 is designed to help FDA-regulated companies obtain the benefits of electronic data management
- Part 11 is designed to prevent fraud while permitting the widest possible use of electronic technology
- Contains detailed guidelines that establish which electronic records and signatures can be considered equivalent to paper records and handwritten signatures
- Part 11 requires (1) controlled access; (2) computer-generated audit trails; (3) electronic digital signatures

Applicability of Part 11

GXP Training
GXP Tracking
SOP Systems

GXP Quality Management Systems

GLP

GCP

GMP

Data Acquisition
Environmental Impact
Laboratory Information Management (LIMS)
Laboratory Robotics
Stability Systems
Toxicology Systems

Adverse Event Reporting
Case Report Form Systems
Centralized Laboratory
Clinical Data management
Clinical Supply Systems
Data Acquisition & Reporting
Remote Data Entry
Statistical Analysis Systems

Manufacturing Execution (MES)
Maintenance Management (MMS)
Calibration Management (MCS)
Facility Management Systems
Enterprise Resource Plan (ERP)
SCADA Systems
Supply Chain Planning (SCP)
Internet Applications
EDI
PLC Systems

What's in a Name?

- CFR – Code of Federal Regulations.
- Part 11 – Deals with Electronic Records and Electronic Signatures.
- GAMP – Good Automated Manufacturing Practice.

21CFR Part 11 and GAMP
WHAT'S THE DIFFERENCE?

GAMP & 21 CFR Part 11

What's the difference?

GAMP is a Guideline

21 CFR

is

LAW

21 CFR Part 11 Benefits

Everything from faster time-to-market for new drugs to reduced cost of mandated recalls can result from the implementation of Part 11 systems.

Elements

Electronic Records

TECHNICAL

- Validation
- Inspect ability
- Security
- Audit Trails

PROCEDURAL

- Qualification
- Accountability
- Documentation

Electronic Signatures

Biometric

Non-Biometric

Validation

- The computerized system shall be validated in accordance with the Corporate Standards and regulatory requirements to ensure:
 - Accuracy
 - Reliability
 - Consistent Intended Performance
 - Ability to discern invalid or altered records

Risk Based Approach to Part 11

The legal, regulatory and practical implications of electronic records. Good electronic records are solid in:

- authenticity
- reliability
- trustworthiness
- integrity
- accessibility as needed

Predicate Rule Requirements

- Provide governance for most regulatory activities within a life sciences organization
- Predicate Rules include:
 - ICH E6 Good Clinical Practices (parts 310, 312, 314)
 - Good Laboratory Practices (21 CFR Part 58)
 - Good Manufacturing Practices (21 CFR Part 210 & 211)
 - Quality System Practice (21 CFR Part 820)

Inspect ability

- Procedures and controls shall be designed and implemented to include the ability to:
 - Generate accurate and complete copies of records in both human and electronics form for inspection, review, and copying by the FDA.
 - Protect records to enable their accurate and ready retrieval throughout the record retention period.

Security

- Security procedures and controls shall be designed and implemented to include:
 - Physical system access shall be limited to authorized individuals.
 - Operational system checks shall enforce the proper sequencing of steps in a process.
 - Logically access the System.
 - Electronically sign a record.
 - Access the operation or computer system input or output device.
 - Alter a record.
 - Perform a specific operation.
 - Device or terminal checks shall determine validity of the source of input or operation.

Audit Trails

- Procedures and controls shall be designed and implemented for audit trails to:
 - Be Sure
 - Be Computer Generated
 - Be time- and date-stamped
 - Record creation of electronic records
 - Record modification of electronic records
 - Record deletion of electronic records
 - Ensure that changes to electronic records shall not obscure previously recorded information
 - Ensure that audit trail records shall be maintained for at least as long as the retention of the underlying
 - Ensure that audit trail records shall be available for FDA review and copying

Qualification

- Determination that the following persons have the education, training, and experience to perform their assigned tasks:
 - Developer(s) of the computerized system
 - Maintainer of the computerized system
 - User(s) of the computerized system

Accountability

- Establishment of, and adherence to, written policies and/or procedures that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter records and signatures falsification.

Documentation

- Establishment and use of appropriate controls over the documentation for system operation and maintenance, to include:
 - Distribution of documentation
 - Access to documentation
 - Use of documentation
 - Revision and change control procedures to maintain an audit trail that documents the time-sequences development and modification of the systems documentation

Open and Closed Systems

- Closed Systems are controlled within the local organization.
- Open Systems are outsourced externally to a system provider. In addition to the requirements for a closed system, there is a requirement to ensure:
 - Authenticity of data.
 - Integrity of data.
 - Confidentiality

Signature Manifestation

- Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:
 - The printed name of the signer
 - The date and time when the signature was executed
 - The meaning of the signature

Signature/Record Linking

- Electronic signatures, and handwritten signatures executed to electronic records, shall be linked to their respective electronics record to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Electronic Signatures - General

- Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
- The identity of the individual shall be verified prior to the organization establishing, assigning, certifying, or otherwise sanctioning that individual's electronic signature.
- Persons using electronic signatures shall, prior to or at the time of such use, certify to the FDA that the electronic signatures used in the computerized system on or after August 20, 1997 are intended to be handwritten signatures.
- The certificate shall be submitted in paper form and signed with a traditional handwritten signature to the appropriate FDA Office specified in the Regulations.

Electronic Signatures

Non-Biometric

- Employ at least 2 distinct identification components such as an identification code and password.
- When an individual executes a series of signing during a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components. Subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by the individual.
- When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.
- Be used only by their genuine owners.

Electronic Signatures

Biometric

- Electronic records based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Identification Codes/Passwords

- Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity, including:
 - The combination of identification code and password shall be unique
 - Identification code and passwords issuance shall be periodically checked, recalled, or revised (e.g. to cover such events as password aging).

Identification Codes/Passwords

- Procedures and controls shall be designed and implemented for devices which bear or generate identification code or password information to:
 - Electronically de-authorize devices that have been lost, stolen, or potentially compromised.
 - Issue temporary or permanent replacements using suitable, rigorous controls.

Identification Codes/Passwords

- Transaction safeguard shall be implemented to:
 - Prevent unauthorized use of identification codes and/or passwords.
 - Detect any attempt at unauthorized use of identification codes and/or passwords.
 - Report in an immediate and urgent manner any attempt at unauthorized use of identification codes and passwords to the system security unit, and, as appropriate, organizational management.
- Initial and periodic testing of devices that bears or generates identification code or password information.

Compliance with Part 11

Part 11 compliance begins with the company having an understand CFR Part 11 and becoming educated about the specific regulations and requirements. The initial steps towards CFR Part 11 compliance includes :

- Defining a set of objectives for achieving compliance
- Communicating the implications of Part 11 for people involved and ensure the commitment to resolve non-compliance
- Creating an interpretation of Part 11
- These basic steps create an awareness of CFR Part 11 compliance within an organization and prepare the organization for changes expected due to CFR Part 11.

Systems Inventory

- The foundation for compliance involves developing an inventory of your organizations hardware and software, and a network architecture document appropriate for your circumstances.
- This is simply knowing what you have and where it's located.

Identify Applicable Systems

Identify the computerized systems in your inventory that fall under the requirement to comply with 21 CFR Part 11. These are the systems that meet the following criteria:

- The process or the applicable data are covered under an existing FDA regulation
- A computerized system is being used to create, modify, maintain, archive, retrieve, or transmit the data

Gap Analysis

- Document what the systems are supposed to do (e.g., functional requirements)
- Document how the systems work (e.g., technical specifications)
- Document the applicability of the specific electronic records/signature provisions, and how the specific requirements of the regulation are being addressed
- Formal test plans and documented test results, with traceability to functional requirements, technical specifications, and appropriate tests of stress/limits boundary conditions
- Evidence of validation (e.g., validation plan, validation summary, installation/operational/performance qualifications)

Gap Analysis

- Organization chart and job descriptions to document the appropriateness of the organization structure
- Policies and procedures (i.e., Standard Operating Procedures [SOPs]) that provide for system validation, development and deploying systems according to a formal methodology, physical and logical security, backup and recovery, system operations, staff training, change control, contingency planning, and use of purchased systems
- Effective audits and inspections of computer systems and related processes by the Quality Assurance (QA) unit

Remediation

- The systems were stratified in order of risk to the company
- Each issue would have been associated with a specific corrective action (e.g., SOPs to be developed, validation activities to be performed, and vendor audits to be conducted)
- Roles and responsibilities, resource requirements, milestones, and target dates were identified
- The plan was reviewed and approved by appropriate representatives of company management, information technology, and QA

Maintaining Compliance

- You are now in the process of implementing appropriate procedures and controls. These are referred to in 21 CFR Part 11 as:
- “...procedures and controls that are designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.”

Veracord®



A Division of **Veracord**

Presented by:

David Park Schutz

park@veracord.com

408.294.5501

www.veracord.com

Mary Kay Lofurno

mklofurno@syberworks.com

www.syberworks.com

52 South First Street Suite 320

San Jose, California 95113

P: 408.294.5500

F: 408.294.5507

www.veracord.com