conformity

keeping it compliant

Regulatory Overview
Annex 11 and Part 11

Sion Wyn
Conformity
+[44] (0) 1492 642622
sion.wyn@conform-it.com

Two Key Regulations

- Annex 11

- 21 CFR Part 11

- Apply to the regulated company, but often have a significant impact on suppliers and service providers…

EU GMP Annex 11

Volume 4, EU Guidelines to Good Manufacturing Practice

Medicinal Products for Human and Veterinary Use

Annex 11 - Computerised Systems

EU GMP - Annex 11

“…the Annex has been revised in response to the increased use of computerised systems and the increased complexity of these systems.”

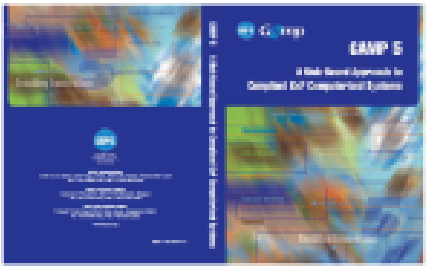
EU GMP Annex 11

- Revised **Annex 11** published January 2011
- Came into effect June 2011
- Adopted by PIC/S: October 2012

The Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme (jointly referred to as PIC/S)

GAMP 5 Alignment

- Life Cycle Concept
  - Project Phase / Operation Phase
  - Application / Infrastructure
- Terminology
  - Process Owner
  - System Owner
- Other good practice aspects…



Scope

- *Applies to all forms of computerised systems used as part of GMP regulated activities.*

Principle

- *…there should be no resultant decrease in product quality, process control or quality assurance.*
- *There should be no increase in the overall risk of the process.*

(A Risk-Based Approach…)

Principle

- *The application should be validated*
- *IT infrastructure should be qualified*

Validation (of Applications)

- Achieving and maintaining compliance and fitness for intended use by:
  - principles, approaches, and life cycle activities within the framework of validation plans and reports
  - application of appropriate operational controls throughout the life of the system

GAMP Interpretation

Qualification (of Infrastructure)

- Control and Compliance
- Initial conformance with established standards through a planned verification process
  - building on good IT practices.
- Control to be maintained by established processes and quality assurance activities
  - effectiveness to be periodically verified.

GAMP Interpretation

More details later…

Risk Management

- *Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality.*

(A Risk-Based Approach…)

Risk Management

- *As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.*

(A Risk-Based Approach…)

Validation

- *Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.*

(A Risk-Based Approach…)

Personnel

- *There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT*
- *All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.*

Suppliers and Service Providers

- ***When*** *third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing…*

Suppliers and Service Providers

- *[**Then**]…formal agreements must exist between the manufacturer and any third parties and these agreements should include clear statements of the responsibilities of the third party.*
- *IT-departments should be considered analogous.*

Suppliers and Service Providers

- Internal providers such as IT departments
  - If covered by overall QMS including policies, procedures, and supporting audits…
  - …then formal contracts not required.

GAMP Interpretation

Suppliers and Service Providers

- Internal providers such as IT departments
  - Agreements such as SLAs and OLAs, as described in ITIL, are useful good practice, but not mandatory.

SLA - Service Level Agreement
OLA - Operational Level Agreement
ITIL - Information Technology Infrastructure Library

GAMP Interpretation

Suppliers and Service Providers

- *The need for an audit should be based on a risk assessment.*
- *Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.*

Suppliers and Service Providers

- Evidence of
  - Appropriate assessment process
  - Subsequent judgement of supplier suitability
  - Significant GMP related findings and outcomes
- …should be made available to regulators on request.

GAMP Interpretation

Suppliers and Service Providers

- Some detailed aspects of assessment finding, especially those related to supplier intellectual property and technology, may be covered by confidentiality agreements.

GAMP Interpretation

Suppliers and Service Providers

- If a regulator requests supplier information, a request may be passed on to the supplier…
- …and when necessary further confidentiality agreements discussed.

GAMP Interpretation

System Description

- *For critical systems an up to date system description detailing the arrangements, data flows and interfaces with other systems or processes, software pre-requisites, and security measures should be available*.

Data Integrity and Security Topics

- Access Control
- Interfaces
- Entry of critical data
- Backups
- Data Migration
- Archiving and long term retention of data

(Consistent with industry good practice…)

Data Migration and Archiving

- *If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.*

Integrity of Interfaces

- *Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.*

Security and Integrity

- *For critical data entered manually, there should be an additional check on the accuracy of the data.*
- *This check may be done by a second operator or by validated electronic means.*

Security and Integrity

- *Data should be secured by both physical and electronic means against damage.*
- *Stored data should be checked for accessibility, readability and accuracy.*
- *Access to data should be ensured throughout the retention period.*

Security and Integrity

- *Regular back-ups of all relevant data...*
- *Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.*

Security and Integrity

- *Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons.*

Security and Integrity

- *Data may be archived.*
- *This data should be checked for accessibility, readability and integrity*.

Audit Trail

- *Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail").*

Audit Trail

- *For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.*

Audit Trail Review

- The need for, and the type and extent of, audit trails should be based on a documented and justified risk assessment. Specific GxP (predicate) requirements requiring audit trails may also apply.

GAMP Interpretation

Audit Trail Review

- As part of normal business process and data integrity review
- As a tool for investigation
- Verification that audit trails are implemented and continue to be effective
- …rather than continuous routine review.

GAMP Interpretation

Audit Trail – Good Practice

- Verification of audit trail functionality (Validation and periodic review)
- Suitable security controls for high risk records
- Segregation of duties, and role-based security
- Established procedures for system use, administration, and change management

GAMP Interpretation

Other Operational Topics

- Periodic Evaluation
- Change Management
- Configuration Management
- Incident Management
- Business Continuity

Electronic Signatures

- *Have the same impact as hand-written signatures within the boundaries of the company,*
- *Be permanently linked to their respective record*
- *Include the time and date that they were applied*

Electronic Signatures

- Allowed – but not mandatory
- Consistent with FDA approach
- Signatures applied to maintained records not subject to European E-Commerce Directives

GAMP Interpretation

21 CFR Part 11


federal register

Thursday
March 20, 1997

Part II

Department of Health and Human Services

Food and Drug Administration

21 CFR Part 11
Electronic Records; Electronic Signatures; Final Rule
Electronic Submissions; Establishment of Public Docket; Notice

13429

ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A--General Provisions

11.1 Scope.

11.2 Implementation.

11.3 Definitions.

Subpart B--Electronic Records

11.10 Controls for closed systems.

11.30 Controls for open systems.

11.50 Signature manifestations.

11.70 Signature/record linking.

Subpart C--Electronic Signature

11.100 General requirements.

11.200 Identification mechanisms and controls.

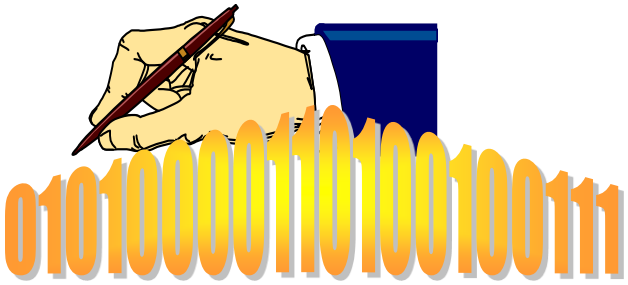
11.300 Controls for identification codes/passwords.

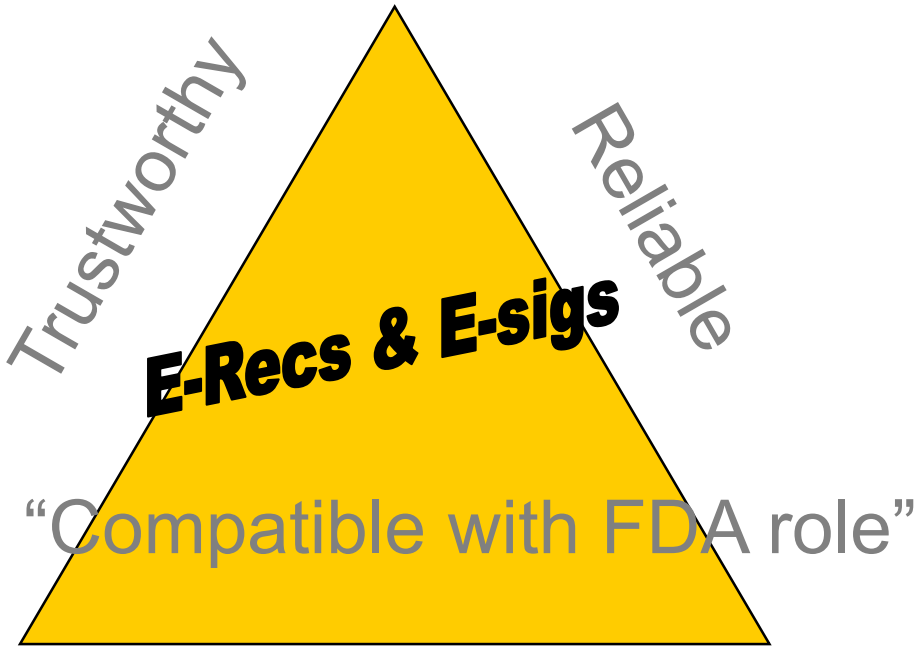
Effective August 20, 1997

Background

- Why was Part 11 required?
- GxP regulations required paper records and paper signatures
- Technology had moved on, and industry wanted to use electronic records and electronic signatures

FDA's Concerns





Electronic records and signatures bring many benefits, but may also bring risks – Part 11 aims to manage such risks

FDA wanted to "Accept and promote new technology whilst maintaining the ability to promote public health"

Scope and Application Guidance

- Problems arose in the interpretation and implementation of the regulation…leading to…
- FDA Decision to re-examine Part 11
  - An element of the FDA 21st Century Initiative
- Part 11 Guidance Published August 2003

Guidance for Industry

Part 11, Electronic Records; Electronic Signatures — Scope and Application

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 Applied Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)

August 2003
Pharmaceutical CGMPs

Scope and Application Guidance

- The Key Messages:
  - Narrow Scope
    - Part 11 applies only to records and signatures required by the US GxP regulations – the “predicate rules” – and maintained electronically
  - Risk Based Controls
    - Specific Part 11 controls should be applied based on a justified and documented risk assessment

Predicate Rules

- Records are required by a “predicate rule”
  - E.g. 21 CFR 210/211 (Pharmaceutical GMPs)
- The predicate rule defines:
  - What records must be maintained
  - The content of records
  - Whether signatures are required
  - How long records must be maintained

Specific Part 11 Requirements

- Validation of Systems
- Access Control
- Authority Checks
- Operational / Device Checks
- Protection of records – retention and copies
- Policies, Training, System Documentation
- E-Signature controls

Detail of requirements will be covered during training course …

Annex 11 vs. Part 11

- Scope and Objectives of the regulations
- Narrowness of scope definitions vs. prescriptive details of controls
- Initial PIC/S and FDA Guidance harmonization
- Allows common approaches and harmonization

conformity

keeping it compliant

Sion Wyn
Conformity
+[44] (0) 1492 642622
sion.wyn@conform-it.com