COMPLIANCE PER DATA INTEGRITY NEI SISTEMI DI AUTOMAZIONE SECONDO GAMP- NORME ED ESEMPI

Andrea Franco

June 2016

TABLE OF CONTENTS

□ A Brief history of “Data Integrity”

□ “Data Integrity” recent deficiencies

□ EU/US relevant current references and New “Data Integrity” Guidelines

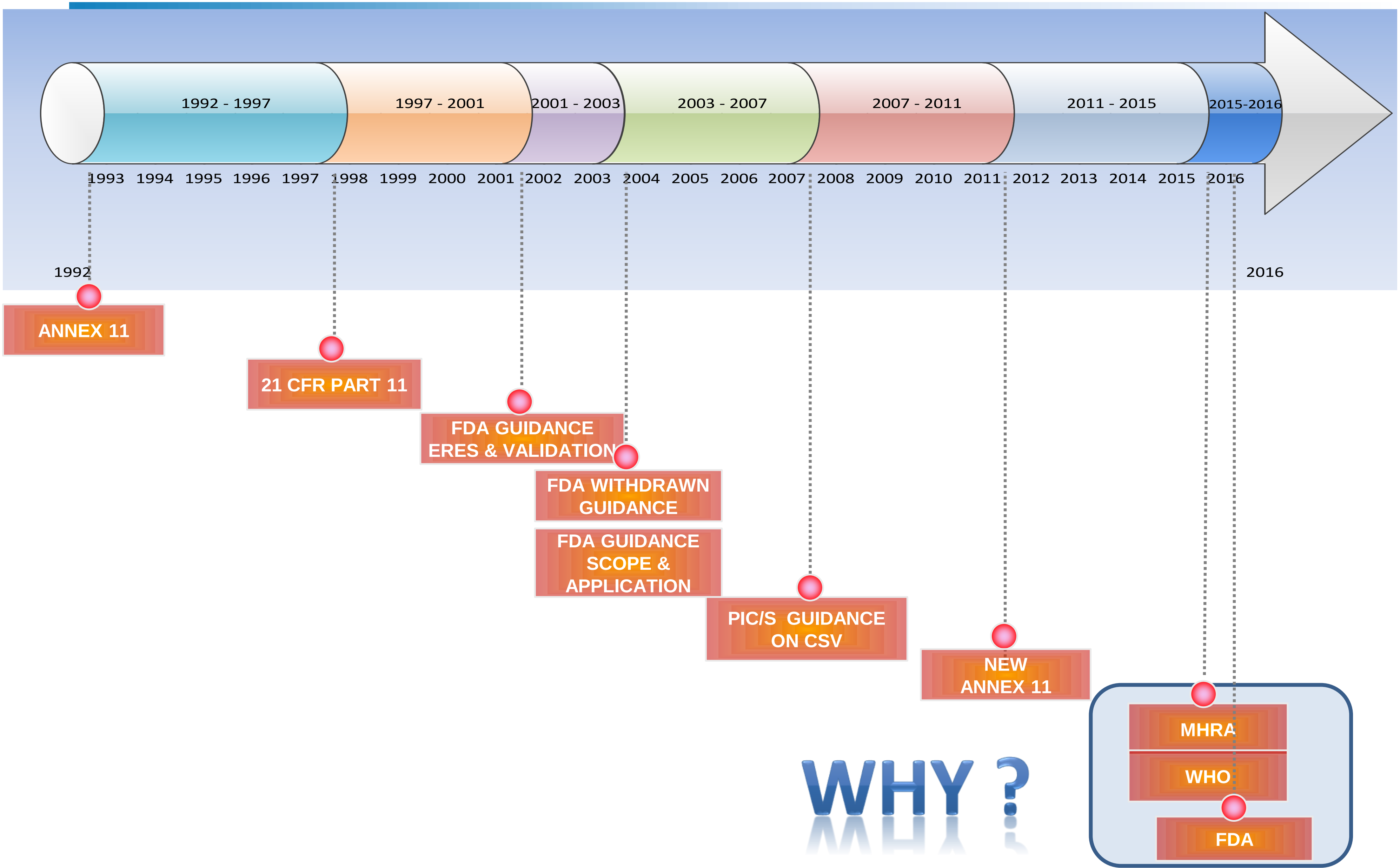
□ Manufacturing Automation Systems

□ Typical Electronic Data in Manufacturing Automation System

□ Attributes for “Data Integrity” applied to Manufacturing Automation Systems

□ Conclusions

A BRIEF HISTORY OF DATA INTEGRITY



1992 - 1997 | 1997 - 2001 | 2001 - 2003 | 2003 - 2007 | 2007 - 2011 | 2011 - 2015 | 2015-2016

1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016

1992

2016

ANNEX 11

21 CFR PART 11

FDA GUIDANCE ERES & VALIDATION

FDA WITHDRAWN GUIDANCE

FDA GUIDANCE SCOPE & APPLICATION

PIC/S GUIDANCE ON CSV

NEW ANNEX 11

MHRA

WHO

FDA

WHY ?

THREE NEW GUIDELINES – WHY ?

- □ Data Integrity has always been a requirement but has recently become a major concern for global regulatory authorities, resulting in a significant increase in regulatory observations in this area.

- □ FDA have issued **a huge number of Warning Letters** to different manufacturers outside US (mainly India and China) in the last 2 years and multiple other Warning Letters to Europe for issues regarding data integrity.

  - □ **Most of Warning Letters** issued between 2013 and 2014 (to non US sites) **had Data integrity issues** and this trend is increasing

- □ (European Medicines Agency) In 2013 **6 statements of non Compliance** related with Data Integrity

- □ (European Medicines Agency) In 2014 **6 statements of non Compliance** (August 2014) related with Data Integrity

EXAMPLE OF FDA DATA INTEGRITY VIOLATIONS (1/2)

Examples of deficiencies in Lab:

□ Warning Letters issued to US based Manufacturer (Mar 2015)

- Your firm failed to exercise appropriate controls over computer or related systems to assure that **only authorized personnel institute changes in master production and control records,**
- Specifically, your **high performance liquid chromatography (HPLC)** and gas chromatography (GC) data acquisition software, TotalChrom®, **did not have sufficient controls to prevent the deletion or alteration of raw data files.** During the inspection, the investigator observed that the server that maintains electronic raw data for HPLC and GC analyses (the J drive) contains a folder named “Test,” and that **chromatographic methods, sequences, and injection data saved into this folder can be deleted by analysts.** The investigator also found that data files initially created and stored in the “Test” folder had been deleted, and that back-up files are overwritten.
- In addition, because **no audit trail function was enabled** for the “Test” folder, your firm was unable to verify what types of injections were made, who made them, or the date or time of deletion. The use of audit trails for computerized analytical instrumentation is essential to ensure the integrity and reliability of the electronic data generated

EXAMPLE OF FDA DATA INTEGRITY VIOLATIONS (2/2)

Examples of deficiencies in Production:

□ Warning Letters issued to India based Manufacturer (Dec 2015)

- You lacked audit trails or other sufficient controls to facilitate traceability of the individuals who access each of the programmable logic controller (PLC) levels or Man-Machine Interface (MMI) equipment.
- You had no way to verify that individuals have not changed, adjusted, or modified equipment operation parameters.
- Password shared by four or five individuals
- you had not established or documented a control program to describe the roles and responsibilities of production equipment system administrators.
- You suggested that traceability to the individual operator could be determined through a hybrid system using the batch manufacturing record and equipment logbook. However, because you used shared login credentials that did not permit identification of a specific person using the shared login, you have not shown how your hybrid system could link specific actions to a specific operator.

EXAMPLE OF DATA INTEGRITY FAILURE BY EMA (HPRA)

HPRA
An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority

Data Integrity: Production Environment
MANUAL AND AUTOMATED SYSTEMS

Ciara Turley

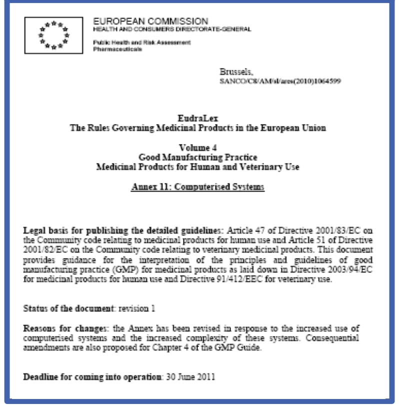
GMP Conference
12th November 2014

Examples of deficiencies in Production:

- □ A **generic operator password** was in use
- □ A **single generic user name and password** was used to access and operate the equipment.
- □ There was **no controlled recipe in place** to confirm that parameter settings on the machine were those approved.
- □ The **time on the HMI was incorrect** – the actual time (taken from the wall clock in the packaging area was recorded at 12:15, the machine time was displayed as 11:08.
- □ **Audit trails were not reviewed**.
- □ The **audit trail could not be generated** at the time of inspection.
- □ The **print out function was not enabled** and there was no assessment to determine if stored data could be securely transferred or downloaded to storage media in an intelligible format for review
- □ The system and **security for archiving of data was not known**
- □ The **User Requirement Specification** did not specifically state all the requirements for the machine and **was not linked to any critical process parameters / variables**

GLOBAL RULE FOR IT COMPLIANCE

Annex 11



EUROPEAN COMMISSION
HEALTH AND CONSUMERS DIRECTORATE-GENERAL

Public Health and Risk Assessment
Pharmaceuticals

Brussels,
SANCO/C8/AM/sl/ares(2010)1064599

EudraLex
The Rules Governing Medicinal Products in the European Union

Volume 4
Good Manufacturing Practice
Medicinal Products for Human and Veterinary Use

Annex 11: Computerised Systems

Legal basis for publishing the detailed guidelines: Article 47 of Directive 2001/83/EC on the Community code relating to medicinal products for human use and Article 51 of Directive 2001/82/EC on the Community code relating to veterinary medicinal products. This document provides guidance for the interpretation of the principles and guidelines of good manufacturing practice (GMP) for medicinal products as laid down in Directive 2003/94/EC for medicinal products for human use and Directive 91/412/EEC for veterinary use.

Status of the document: revision 1

Reasons for changes: the Annex has been revised in response to the increased use of computerised systems and the increased complexity of these systems. Consequential amendments are also proposed for Chapter 4 of the GMP Guide.

Deadline for coming into operation: 30 June 2011

- **TERRITORY**: EU Community Market
- **TARGET**: Computerized Systems
- **LEGAL BASIS**: This document provides guidance for the interpretation of the principles and guidelines of good manufacturing practice (GMP) for medicinal products as laid down in Directive 2003/94/EC for medicinal products for human use and Directive 91/412/EEC for veterinary use.
- **ULTIMATE PURPOSE**: Where a computerized system replaces a manual operation, there should not be a resultant decrease in product quality, process control or quality assurance
- **REGULATORY SCOPE**: GMP Pharma & Veterinary
- **EFFECTIVE DATE**: June 2011

21 CFR Part 11

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

- **TERRITORY**: US Market
- **TARGET**: Computerized Systems
- **LEGAL BASIS**: Section of the US Law which applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act
- **ULTIMATE PURPOSE**: To set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.
- **REGULATORY SCOPE**: GxP
- **EFFECTIVE DATE**: August 1997

US 21 CFR Part 11 & EU GMP Annex 11 are the equivalent Global standards

SIMILAR TO

CHINA CFDA Computer Rule

BRASIL Anvisa Title VII: Computer information systems

CANADA Health PIC/S Annex 11: Computerised Systems

AGENCIES REACTIONS

□ Due to the recurrent inspectional findings, almost every Regulatory Agency has provided guidances to the Pharmaceutical firms oriented to

- Clarify Regulatory expectations
- Prevent Data Integrity violations

2015-2016 NEW GUIDELINES

MHRA

MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015

Introduction:

Data integrity is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality. This document provides MHRA guidance on GMP data integrity expectations for the pharmaceutical industry. This guidance is intended to complement existing EU GMP relating to active substances and dosage forms, and should be read in conjunction with national medicines legislation and the GMP standards published in Eudralex volume 4.

The data governance system should be integral to the pharmaceutical quality system described in EU GMP chapter 1. The effort and resource assigned to data governance should be commensurate with the risk to product quality, and should also be balanced with other quality assurance resource demands. As such, manufacturers and analytical laboratories are not expected to implement a forensic approach to data checking on a routine basis, but instead design and operate a system which provides an acceptable state of control based on the data integrity risk, and which is fully documented with supporting rationale.

Data integrity requirements apply equally to manual (paper) and electronic data. Manufacturers and analytical laboratories should be aware that reverting from automated / computerised to manual / paper-based systems will not in itself remove the need for data integrity controls. This may also constitute a failure to comply with Article 23 of Directive 2001/83/EC, which requires an authorisation holder to take account of scientific and technical progress and enable the medicinal product to be manufactured and checked by means of generally accepted scientific methods.

Throughout this guidance, associated definitions are shown as hyperlinks.

Establishing data criticality and inherent integrity risk:

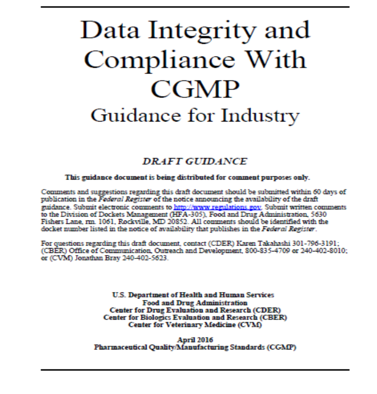
In addition to an overarching data governance system, which should include relevant policies and staff training in the importance of data integrity, consideration should be given to the organisational (e.g. procedures) and technical (e.g. computer system access) controls applied to different areas of the quality system. The degree of effort and resource applied to the organisational and technical control of data lifecycle elements should be commensurate with its criticality in terms of impact to product quality attributes.

Data may be generated by (i) a paper-based record of a manual observation, or (ii) in terms of equipment, a spectrum of simple machines through to complex highly configurable computerised systems. The inherent risks to data integrity may differ depending upon the degree to which data (or the system generating or using the data) can be configured, and therefore potentially manipulated (see figure 1).

Medicines and Healthcare
Products Regulatory Agency

*"This document provides MHRA **guidance on GMP data integrity expectations for the pharmaceutical industry.** This guidance is intended to complement existing EU GMP relating to active substances and dosage forms, and should be read in conjunction with national medicines legislation and the GMP standards published in Eudralex volume 4"*

FDA



Data Integrity and
Compliance With
CGMP
Guidance for Industry

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Comments and suggestions regarding this draft document should be submitted within 60 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to http://www.regulations.gov. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 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*.

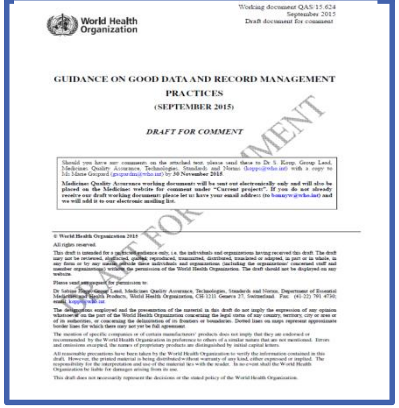
For questions regarding this draft document, contact (CDER) Karen Takahashi 301-796-3191; (CBER) Office of Communication, Outreach and Development, 800-835-4709 or 240-402-8010; or (CVM) Jonathan Bray 240-402-5623.

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 Veterinary Medicine (CVM)

April 2016
Pharmaceutical Quality/Manufacturing Standards (CGMP)

*"The purpose of this guidance is to **clarify the role of data integrity in current good manufacturing practice** (CGMP) for drugs, as required in 21 CFR parts 210, 211, and 212"*

WHO



World Health
Organization

Working document QAS/15.624
September 2015
Draft document for comment

GUIDANCE ON GOOD DATA AND RECORD MANAGEMENT PRACTICES
(SEPTEMBER 2015)

DRAFT FOR COMMENT

Should you have any comments on the attached text, please send these to Dr S. Kopp, Group Lead, Medicines Quality Assurance, Technologies, Standards and Norms (kopps@who.int) with a copy to Ms Marie Gaspard (gaspardm@who.int) by **30 November 2015**.

Medicines Quality Assurance working documents will be sent out electronically only and will also be placed on the Medicines website for comment under "Current projects". If you do not already receive our draft working documents please let us have your email address (to bonnyw@who.int) and we will add it to our electronic mailing list.

DRAFT FOR COMMENT

© World Health Organization 2015

All rights reserved.

This draft is intended for a restricted audience only, i.e. the individuals and organizations having received this draft. The draft may not be reviewed, abstracted, quoted, reproduced, transmitted, distributed, translated or adapted, in part or in whole, in any form or by any means outside these individuals and organizations (including the organizations' concerned staff and member organizations) without the permission of the World Health Organization. The draft should not be displayed on any website.

Please send any request for permission to:

Dr Sabine Kopp, Group Lead, Medicines Quality Assurance, Technologies, Standards and Norms, Department of Essential Medicines and Health Products, World Health Organization, CH-1211 Geneva 27, Switzerland. Fax: (41-22) 791 4730; email: kopps@who.int.

The designations employed and the presentation of the material in this draft do not imply the expression of any opinion whatsoever on the part of the World Health Organization concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. Dotted lines on maps represent approximate border lines for which there may not yet be full agreement.

The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by the World Health Organization in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by the World Health Organization to verify the information contained in this draft. However, the printed material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the World Health Organization be liable for damages arising from its use.

This draft does not necessarily represent the decisions or the stated policy of the World Health Organization.

*"These guidelines highlight, and in some instances clarify, the **application of data management procedures.** The focus is on those principles that are implicit in existing WHO guidelines and that if not robustly implemented can impact on **data reliability and completeness** and undermine the robustness of decision making based upon that data".*

KEY DEFINITIONS (1/4)

TERM	MHRA	WHO	FDA
DATA INTEGRITY	The extent to which all data are complete, consistent and accurate throughout the data lifecycle.	Data integrity is the degree to which a collection of data is complete, consistent and accurate throughout the data lifecycle. The collected data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices.	Data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA)
DATA	Information derived or obtained from raw data (e.g. a reported analytical result)	Data means all original records and certified true copies of original records, including source data and metadata and all subsequent transformations and reports of this data, which are recorded at the time of the GxP activity and allow full and complete reconstruction and evaluation of the GxP activity. Data should be accurately recorded by permanent means at the time of the activity. Data may be contained in paper records (such as worksheets and logbooks), electronic records and audit trails, photographs, microfilm or microfiche, audio- or video-files or any other media whereby information related to GxP activities is recorded	Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

KEY DEFINITIONS (2/4)

TERM	MHRA	WHO	FDA
METADATA	Metadata is data that describe the attributes of other data, and provide context and meaning. Typically, these are data that describe the structure, data elements, inter-relationships and other characteristics of data. It also permits data to be attributable to an individual.	Metadata are data about data that provide the contextual information required to understand those data. Typically, these are data that describe the structure, data elements, interrelationships and other characteristics of data. They also permit data to be attributable to an individual. For example, in weighing the number 8 is meaningless without metadata, i.e. the unit, mg. Other examples of metadata may include the time/date stamp of the activity, the operator ID of the person who performed the activity, the instrument ID used, processing parameters, sequence files, audit trails and other data required to understand data and reconstruct activities.	Metadata is the contextual information required to understand data. A data value is by itself meaningless without additional information about the data. Metadata is often described as data about data. Metadata is structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data. For example, the number "23" is meaningless without metadata, such as an indication of the unit "mg." Among other things, metadata for a particular piece of data could include a date/time stamp for when the data were acquired, a user ID of the person who conducted the test or analysis that generated the data, the instrument ID used to acquire the data, audit trails, etc.
RAW DATA	Original records and documentation, retained in the format in which they were originally generated (i.e. paper or electronic), or as a 'true copy'. Raw data must be contemporaneously and accurately recorded by permanent means. In the case of basic electronic equipment which provides only a printed data output (e.g. balance or pH meter), the printout constitutes the raw data.	No clear definitions available Source data included in the definition of data.	No clear definitions available

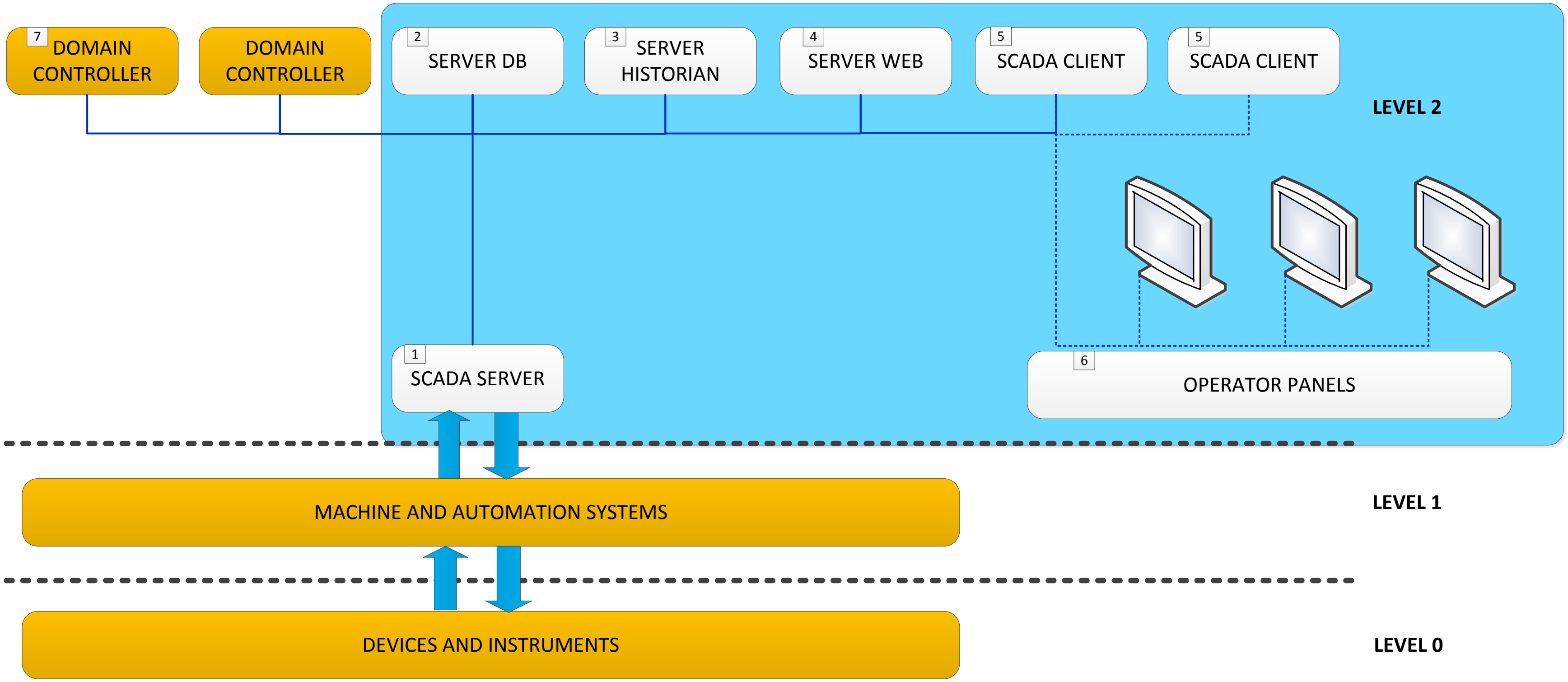
KEY DEFINITIONS (3/4)

TERM	MHRA	WHO	FDA
AUDIT TRAILS	Audit trails to show all changes to the data while retaining previous and original data. It should be possible to associate all changes to data with the persons making those changes, and changes should be time stamped and a reason given. Users should not have the ability to amend or switch off the audit trail	An audit trail is a process that captures details such as additions, deletions, or alterations of information in a record, either paper or electronic, without obscuring or over-writing the original record Computer generated audit trails shall retain the original entry and document the user ID, time/date stamp of the action, as well as a reason for the action, as required to substantiate and justify the action. Computer-generated audit trails may include discrete event logs, history files, database queries or reports or other mechanisms that display events related to the computerized system	Audit trail means a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. An audit trail is a chronology of the “who, what, when, and why” of a record. … Electronic audit trails include those that track creation, modification, or deletion of data (such as processing parameters and results) and those that track actions at the record or system level (such as attempts to access the system or rename or delete a file).
DATA LIFE CYCLE	All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, data retention, archive / retrieval and destruction.	A planned approach to assessing and managing risks to data in a manner commensurate with potential impact on patient safety, product quality and/or the reliability of the decisions made throughout all phases of the process by which data is created, processed, reviewed, analyzed and reported, transferred, stored and retrieved, and continuously monitored until retired	No indications

KEY DEFINITIONS (4/4)

	MHRA	WHO	FDA
COMPUTERIZED SYSTEM	- No definition	A computerized system collectively controls the performance of one or more automated business processes. It includes computer hardware, software, peripheral devices, networks, personnel and documentation, e.g. manuals and standard operating procedures	Computer or related systems can refer to computer hardware, software, peripheral devices, networks, cloud infrastructure, operators, and associated documents (e.g., user manuals and standard operating procedures)
VALIDATION	Computerised systems should comply with the requirements of EU GMP Annex 11 and be validated for their intended purpose.	"implementation and confirmation during validation of computerized systems that all necessary controls for good documentation practices for electronic data are in place and that the probability of the occurrence of errors in the data is minimized"	The collection and evaluation of data … which establishes scientific evidence that a process is capable of consistently delivering quality products

AUTOMATION SYSTEM FOR MANUFACTURING (1/5)



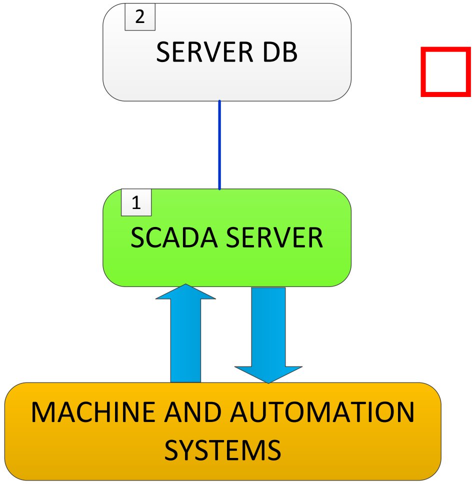
□ MAIN FUNCTIONS

- [1] … [7] Access Control and Security of information
- [1] Recipe Management
- [1] Alarm monitoring and controls
- [2] Recording and monitoring of process parameters
- [3] Archiving of process parameters
- [4] Printing of ERs

□ MAIN ELECTRONIC RECORDS

- [1] [2] Recipes (Static)
- [2] [3] Trends (Dynamic)
- [1] [2] Alarms (Static)
- [3] Process Results (Static)

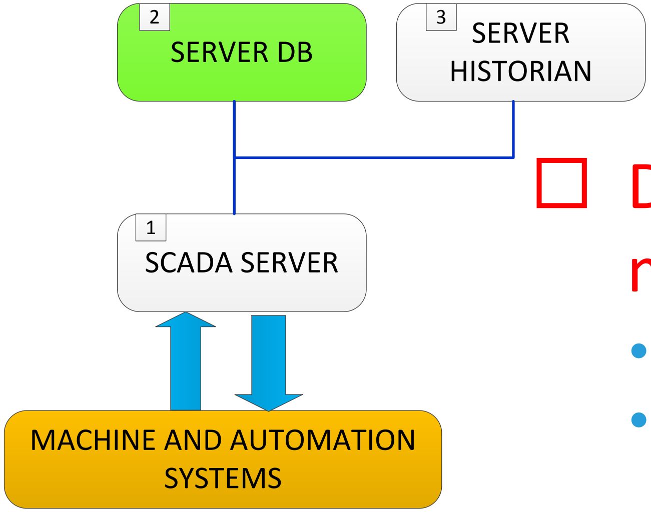
AUTOMATION SYSTEM FOR MANUFACTURING (2/5)



□ SCADA SERVER – typical functions

- Communication with machines/equipment and real-time database data with information exchanged between level 1 and level 2.
- Capturing and Recording of alarms on the Database Server
- Capturing and Recording of process variables (Trends) on the Database Server
- Management of process sequences (Recipes)
- Recording of process events included in the reports on the Database Server
- Monitoring and Diagnostic functions on the network
- Alarm Management – Real Time

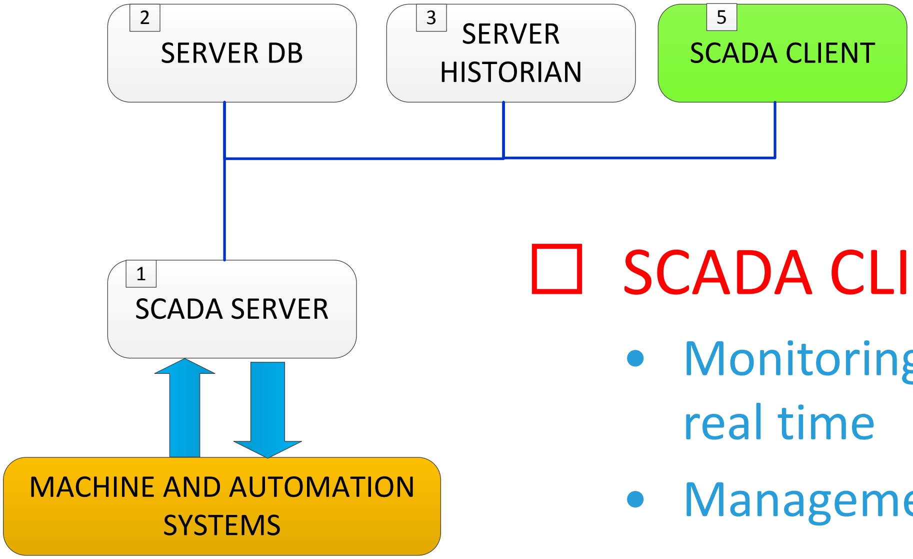
AUTOMATION SYSTEM FOR MANUFACTURING (3/5)



□ DB SERVER DB, where these (typical) data are maintained:

- TREND: process values recorded by the system
- Historical ALARMS: alarms detected by the system and related notes / comments (if any)
- Historical EVENTS: access to the systems and system operations
- AUDIT TRAIL
- GENERAL PARAMETERS: parameters used by more than one recipe
- RECIPES: it contains recipe data and relevant recipe-specific parameters
- PROCESS EVENTS: process events related to the execution of a recipe
- APPLICATION DATA: configurations and settings used by the applications

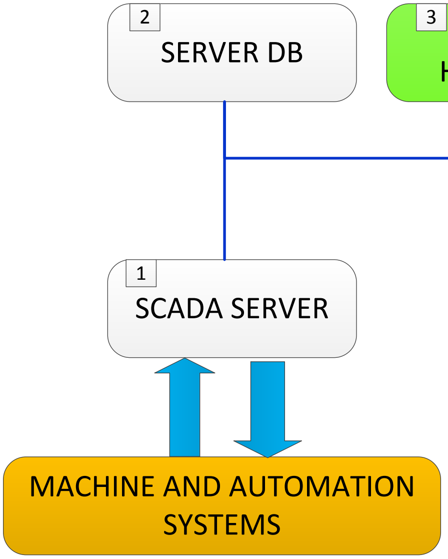
AUTOMATION SYSTEM FOR MANUFACTURING (4/5)



□ SCADA CLIENT – typical functions

- Monitoring of the plant through animated graphical pages in real time
- Management of devices
- Management of general parameters
- Management of Process Recipes
- Alarm Managements
- Display of Graphical Trends
- Display of Audit Trail
- Display of Historical Alarms
- Display of Historical Events
- Display of Process Reports

AUTOMATION SYSTEM FOR MANUFACTURING (5/5)



□ HISTORIAN - typical functions

It contains historical data (trend) managed by the system.

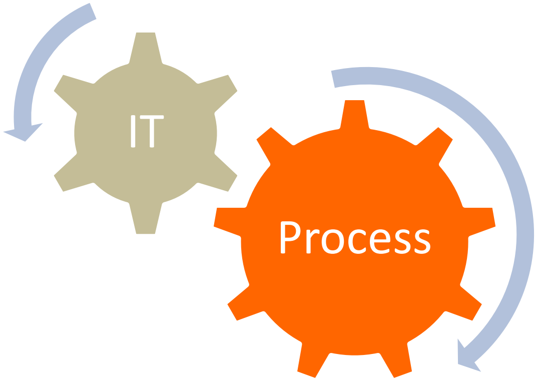
The SW module to display the trend allows to:

- Select a group of process parameters
- Select specific process units
- Zoom specific trend areas
- Move the pointer within the trend
- Select a temporal window
- Export data
- Print the trend

ELECTRONIC RECORDS – SCADA SYSTEMS

Electronic records usually managed by a SCADA system

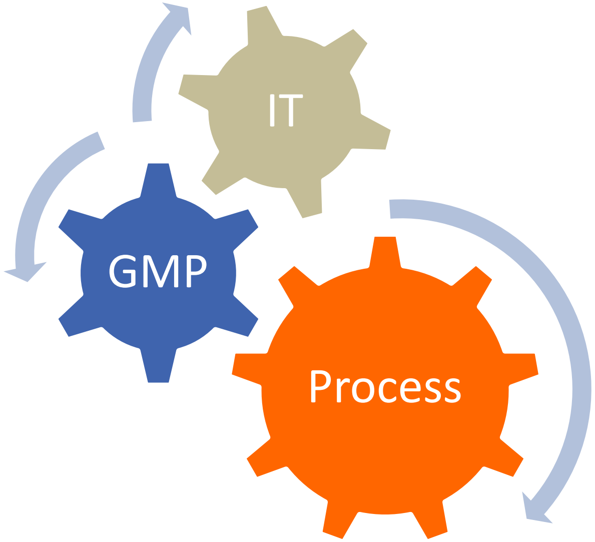
Record	Description
Trends of environmental and process parameters	Pressure, Temperature and Relative Humidity values
Recipe	Process steps in a predefined sequence
Alarm Log	Alarms generated by the system
No Impact Set-Points	Field level automation data settings (i.e. valve or shutter opening rate, fan speed, etc)
Critical Alarm Set-Points	Admitted thresholds of critical environmental parameters aimed at avoiding OOS conditions



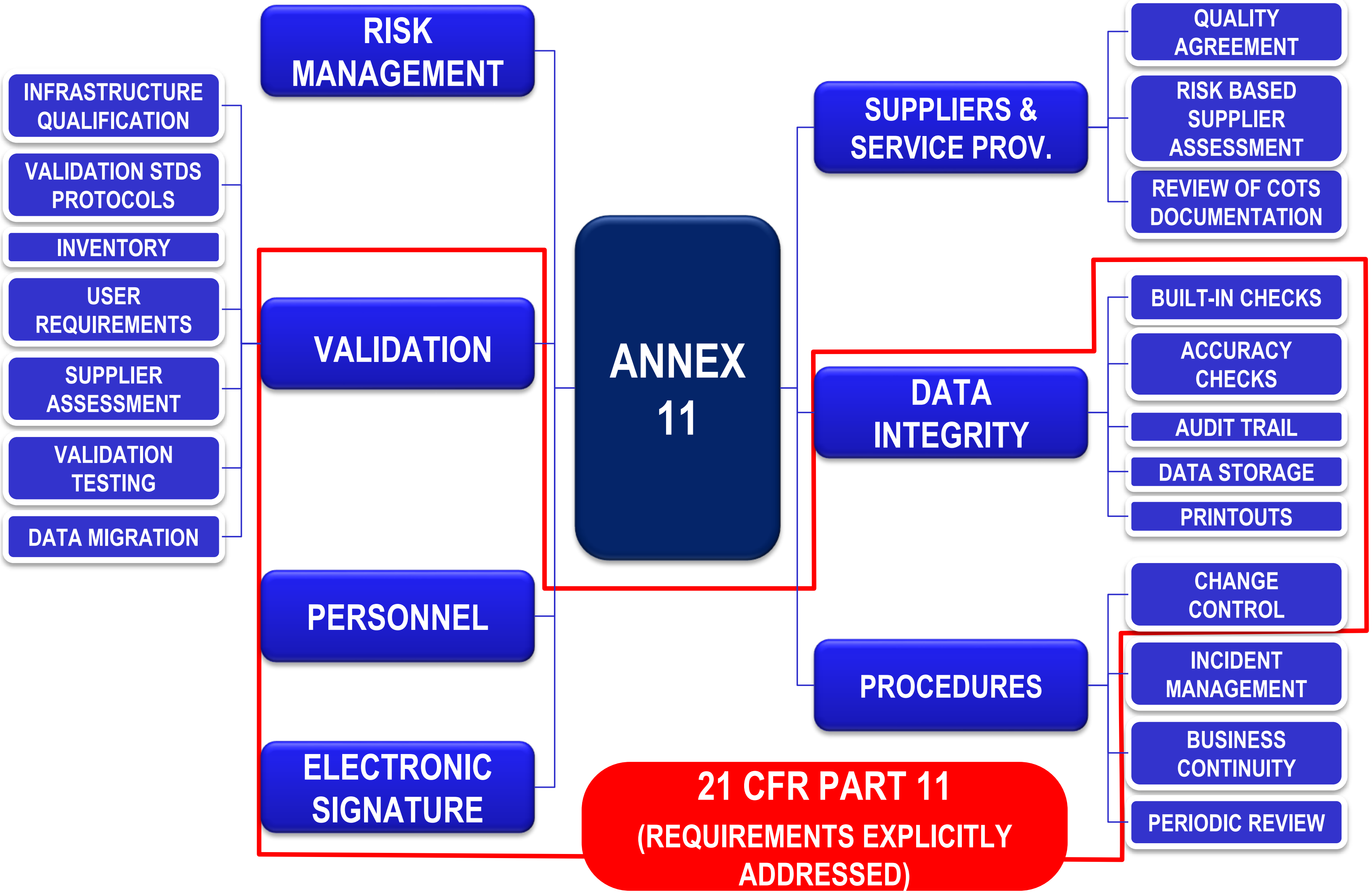
REGULATED ELECTRONIC RECORDS – SCADA SYSTEMS

GMP Electronic records usually managed by a SCADA system

Record	Predicate Rule	GMP
Trends of process or environmental parameters	211.42 (b) (c); 211.68 (a); 211.180 (a); 211.188	**YES**
Recipe	211.100 (b)	**YES**
Alarm Log	211.42 (b) (c); 211.68 (a); 211.180 (a); 211.188	**YES**
No Impact Set-Points	---	**NO**
Critical Alarm Set-Points	211.42 (b) (c); 211.68 (a); 211.180 (a); 211.188	**YES**



ANNEX 11 vs 21 CFR PART 11 MIND MAPS



ULTIMATE PURPOSE OF COMPUTER REGULATIONS

21 CFR Part 11

federal register

Thursday
March 20, 1997

Part II

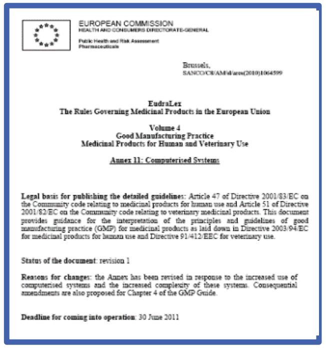
Department of Health and Human Services

Food and Drug Administration

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

ULTIMATE PURPOSE

Annex 11



EUROPEAN COMMISSION
HEALTH AND CONSUMERS DIRECTORATE-GENERAL

Public Health and Risk Assessment
Pharmaceuticals

Brussels,
SANCO/CR/AM/sl/ares(2010)1064599

EudraLex
The Rules Governing Medicinal Products in the European Union

Volume 4
Good Manufacturing Practice
Medicinal Products for Human and Veterinary Use

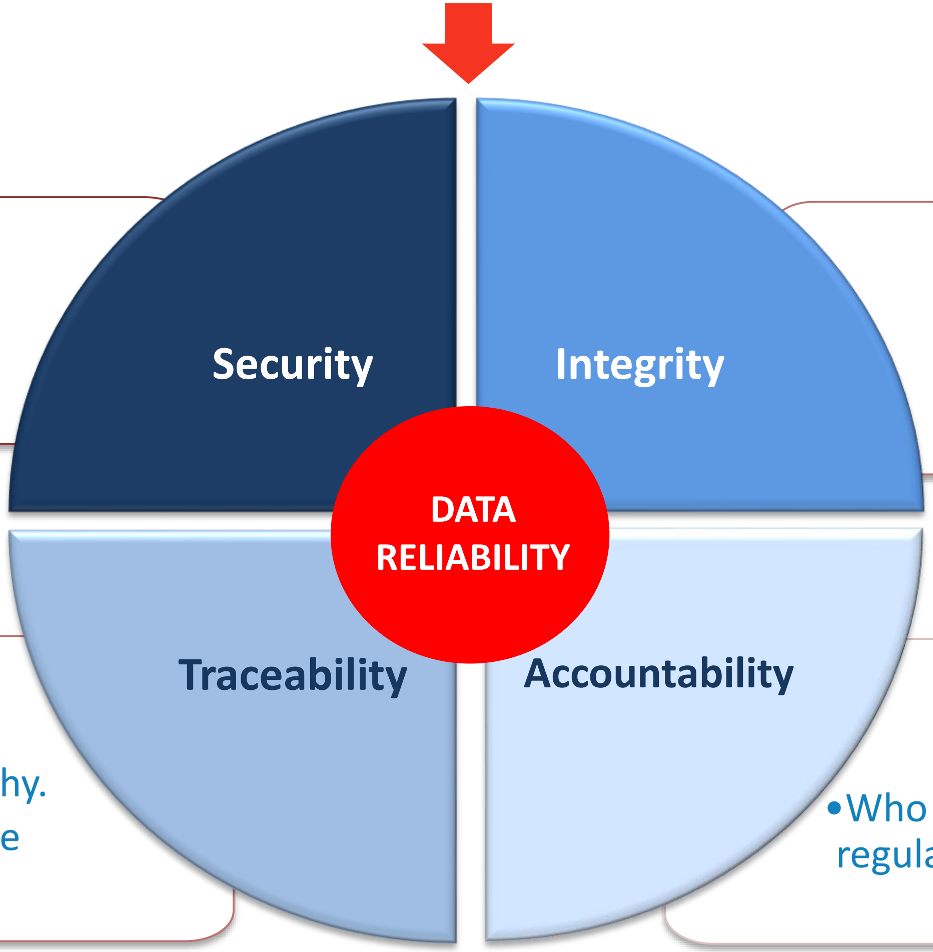
Annex 11: Computerised Systems

Legal basis for publishing the detailed guidelines: Article 47 of Directive 2001/83/EC on the Community code relating to medicinal products for human use and Article 51 of Directive 2001/82/EC on the Community code relating to veterinary medicinal products. This document provides guidance for the interpretation of the principles and guidelines of good manufacturing practice (GMP) for medicinal products as laid down in Directive 2003/94/EC for medicinal products for human use and Directive 91/412/EEC for veterinary use.

Status of the document: revision 1

Reasons for changes: the Annex has been revised in response to the increased use of computerised systems and the increased complexity of these systems. Consequential amendments are also proposed for Chapter 4 of the GMP Guide.

Deadline for coming into operation: 30 June 2011



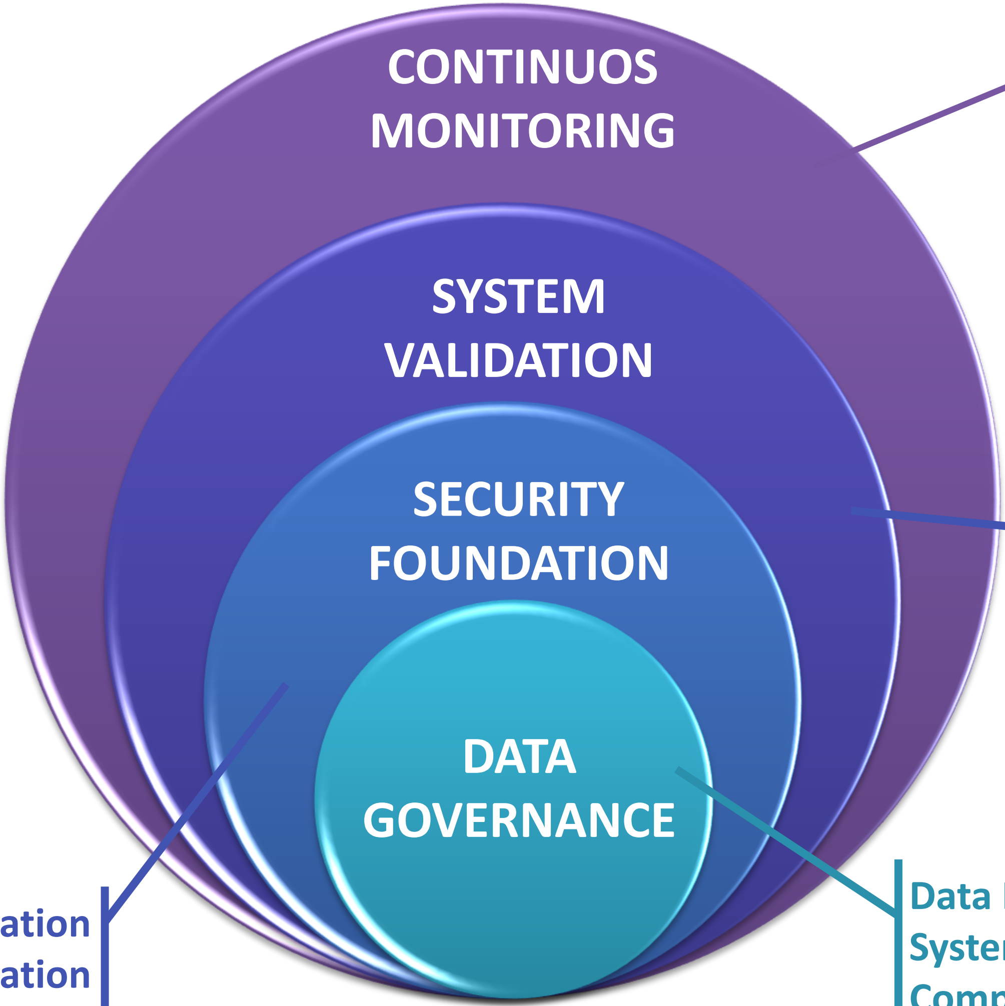
- Access Control
- Authority Check

- Link Raw Data and Result
- Prevent Data Alteration
- Archiving
- Backup
- Critical Process Steps

- Change Control
- Printout and eCopies
- Who did what, when and why.
- Previous entries must not be obscured (Audit trail)

- Who is Accountable from a regulatory perspective?

DATA INTEGRITY PILLARS



Process Supervision
Audit Trail Review
Internal Audit
Periodic Review

System Intended Use Verification
Security implementation
Documented Evidence of System Compliance
Data Integrity Verification

Security implementation
Configuration
User Profiling

Data Integrity Policy
System Inventory
Computer Validation Policy
Staff Training
Historical Data Integrity Assessment

ULTIMATE REQUIREMENT: REGULATORY RECORDS ARE ALCOA (1/3)

PQE

Security

- Access Control
- Authority Check

Traceability

- Change Control
- Who did what, when and why.
- Previous entries must not be obscured

ALCOA	ELECTRONIC CONTROL	AUTOMATION SYSTEMS AND RELATED FUNCTIONS
ATTRIBUTABLE	• Electronic Sign-In – Log ons • Access Control: historical information regarding user access level is available. • Electronic Signature (where used) with associated meaning (Author / Review) • Effective segregation of duties and related role-based security • Audit Trail for create / modify / delete	• Login – Logout capabilities • Access log and query / filter functions • Electronic Signature (single or double) associated to predefined reasons (e.g. Approval) • User Rights Definition • Event Logs • Segregation of Areas and Data • Audit Trail for process and administrative operations
LEGIBLE, TRACEABLE, PERMANENT	• Archiving, Keeping all records • Controls on sequence of events • Time Stamped - Audit Trails • Controls on overwriting • Controls on hidden fields or voided records (access control, audit trail records) • Controls on voiding records.	• Long term archiving of process variables through Historian Server • Sequence can be defined within versioned Recipes • Audit Trail for process and administrative operations (printable / exportable, filter functions) • Configuration settings that limit access to enhanced security rights • Readable Printing Functions • Export of Data in standard electronic format and store in other memory devices. • Display of data in real time ([illegible])

ULTIMATE REQUIREMENT: REGULATORY RECORDS ARE ALCOA (2/3)

Integrity

- Link Raw Data and Result
- Prevent Data Alteration

ALCOA	ELECTRONIC CONTROL	AUTOMATION SYSTEMS AND RELATED FUNCTIONS
ORIGINAL	• Electronic Backup and verification in place, either manual or by use of an automated tool • Back-up logs are often maintained but have not been seen in the past as GMP records. • Archiving records should be locked such that they cannot be altered or deleted without detection and audit trail. The archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period. • Review of Electronic Data • Review of Audit Trail	• Backup can be defined with internal application functions or through "infrastructure tools". • Archiving and Retrieval of information from the Database Server or from the Historian Server • Servers Access Controls and Segregation of Duty prevents data alteration • Metadata are maintained together with raw data (e.g. Trend) • Recipe can be reviewed and approved according to pre-defined workflow (numbers of a roles of reviewer / approver) • Audit Trail can be filtered for specific pre-defined "critical" operations – this makes easier and effective the review.
ACCURATE – "correct, truthful, valid and reliable"	• Records review confirms the accuracy, completeness, content and meaning of the record or documented verification that the printed records are representative of original records (preserving all accuracy, completeness, content and meaning)	• Recipe can be reviewed and approved according to pre-defined workflow (numbers of a roles of reviewer / approver) • Audit Trail can be filtered for specific pre-defined "critical" operations – this makes easier and effective the review. • Trends are stored and archived together with the related metadata • Data are recorded in Database and Archiving System without any human operation.

ULTIMATE REQUIREMENT: REGULATORY RECORDS ARE ALCOA (3/3)

- Change Control
- Who did what, when and why.
- Previous entries must not be obscured

Traceability

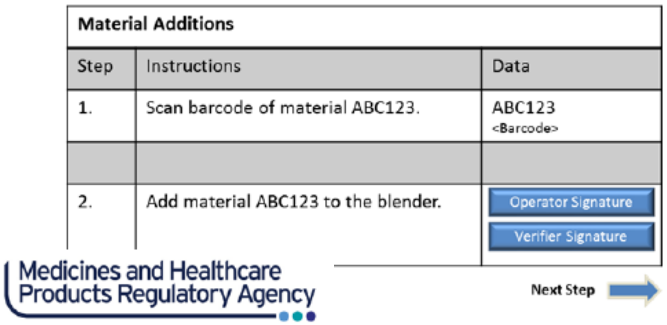
Accountability

- Who is Accountable from a regulatory perspective?

ALCOA	ELECTRONIC CONTROL	AUTOMATION SYSTEMS AND RELATED FUNCTIONS
CONTEMPORANEOUS	• Time and date stamps from system clock – networked or standalone, operating or server clock Time and date stamps are more easily adjusted on un-networked systems. • Synchronization of clock between systems • Locking of clocks on PCs if data is captured locally	• Secure system time/date stamps that cannot be altered by personnel • Time/date stamps can be synchronized across the GxP operations • It is possible discerning of the timing of one activity relative to another (e.g. time zone controls). • Sequence can be defined within versioned Recipes • Critical processing step can be defined within the recipe with parameter that must be within an appropriate limit, range.. • An authorized signer can be accountable of each step (contemporaneous)

Figure 2: Logical design permitting contemporaneous recording of addition of a single material in a manufacturing 'unit of work'. This record is permanently recorded (step 2), with audit trail, before progressing to next 'unit of work'.

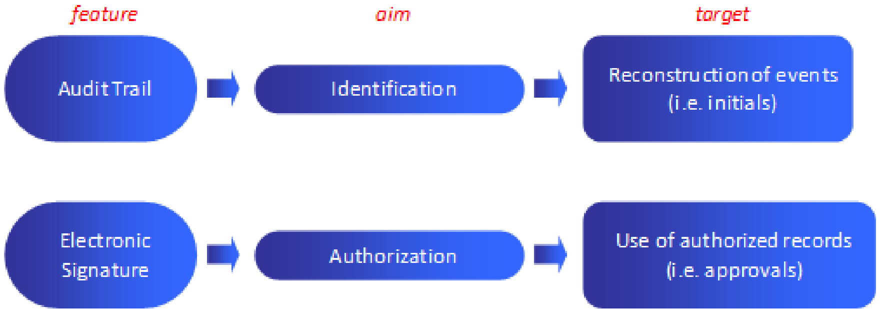
Allows for contemporaneous recording of the material addition by the operator and verifier.



Material Additions		
Step	Instructions	Data
1.	Scan barcode of material ABC123.	ABC123 <Barcode>
2.	Add material ABC123 to the blender.	Operator Signature Verifier Signature

Medicines and Healthcare Products Regulatory Agency

Accountable ≠ Attributable


feature
aim
target
Audit Trail
Identification
Reconstruction of events (i.e. initials)
Electronic Signature
Authorization
Use of authorized records (i.e. approvals)

CONCLUSIONS

□ Prevent Data Integrity Violation through system functionalities

□ Meet the current Regulatory expectations:

- Identify regulated electronic Records & Signatures
- Implement control measures
- Verify reliability of control measures within Validation process
- Monitor effectiveness of these control measures

□ Routinely verify the adequacy of records content (e.g. Audit Trail review)

WHO Guidance:

Implementation and confirmation during validation of computerized systems that all necessary controls for good documentation practices for electronic data are in place and that the probability of the occurrence of errors in the data is minimized;

Andrea Franco
Project Manager

+39 348 802 74 59

a.franco@pqe.eu

florenceromemilanbarcelonagdansk

PHARMA QUALITY EUROPE