



FDA

U.S. Department of Health and Human Services
Food and Drug Administration

ISCT Cell Therapy Liaison Meeting

AABB Headquarters in Bethesda, MD

David Doleski, Team Leader, Branch 2

Division of Manufacturing and Product Quality (DMPQ)

Office of Compliance and Biologics Quality (OCBQ)

Center for Biologics Evaluation and Research (CBER)

September 10, 2009

Regulatory Considerations for the Use of Software for Manufacturing HCT/P

CBER / DMPQ Responsibilities

- Reviews
 - INDs, BLAs, PMAs, NDAs, 510(k)s, Supplements (PAS, CBE-30, CBE), Annual Reports
- Inspections
 - Pre-Approval Inspections, Pre-License Inspections, Sometimes Biennial
- Type C Meetings
 - New Facility Plans, Major Renovations, Automation Issues
- Policy and Guidance
 - Representation on Many Committees, Including FDA Part 11 Committee

Software Lifecycle

- Planning
 - Validation Planning
 - Risk Assessment
 - User Requirements Analysis
 - System Specifications
- Development
 - Design
 - Software Coding
 - Incremental Testing
- Verification/Validation
 - Formal Testing of Software Modules
 - Testing of Software in Actual Manufacturing Environment
- Maintenance
 - Change Control, Possible Revalidation

Software Complexity

Affected By:

- Network/Stand Alone
- Connections to Equipment
- Number of Inputs/Outputs
- Number of Human/Machine Interfaces
- Number of Recipes
- Range of Functionality
- Diversity of Data Types
- Store Data vs. Monitoring vs. Controlling
- Synchronization Requirements

Criticality of Software

Does the Software Impact:

- Process Parameters (e.g. Temperature, Speed, Flow Rate)?
- Sequence of Steps?
- Product Quality?
- Product Identification (Patient ID)?
- Testing and/or Results?
- Quality Decisions (Release/Quarantine)?
- Transmission, Creation, Modification, Maintenance, Archival, Retrieval of CGMP Data?

Examples of Computer Software

Manufacturing Environment:

- Process Monitoring and Control (Distributed Control Systems)
- Environmental Monitoring and Control (Building Monitoring Systems)
- Databases: Quality Systems (Tracking Deviations, Change Control, Investigations)
- Databases: Laboratory Information Management Systems
- Materials Management/ Resource Planning Systems
- Automated Visual Inspection Systems
- Tracking of Stored Samples

Software Categories

GAMP Classification*

1. Infrastructure Software (Windows, UNIX, network monitoring, Anti-Virus)
2. Firmware (Bar Code Scanners, Scales)
3. Non-Configured Products (Some COTS, Proprietary Software, Lab. Instrument Software, Statistical Software, Controllers with Default Settings)
4. Configured Products (SCADA, LIMS, DCS, ERP)
5. Custom Applications (SAP, C++ Code, Manufacturing Recipes)

*ISPE – Good Automated Manufacturing Practices

Software: Assessing Risk

Examples of Approaches:

- ICH Q9 - Quality Risk Management
- ISO 14971:2007 - Medical Devices: Application of Risk Management to Medical Devices
- ISO/IEC 16085-2006: Systems and Software Engineering - Life Cycle Processes - Risk Management
- ANSI/AAMI/IEC 62304:2006 - Medical Device Software: Software Life Cycle Processes
- ISPE GAMP – Guideline for Risk Assessment
- Failure Mode Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)

Computer Systems Integration

Possible Issues with Integrating Multiple Computer Systems Due to Differences in:

- Data, Objects, Processes
- Timing of Data Updates
- Underlying Business Rules
- Quality of Data
- Data Standards
- Communication Methods

Levels/Types of Testing

A Few Types:

- Unit, Subsystem, System, Integration Testing
- Sequence Testing
- Factory Acceptance Testing (FAT)
- Site Acceptance Testing (SAT)
- Alarm Testing
- Boundary Testing
- Network Testing
- Process/Product-Specific Recipes
- User Acceptance Testing

How Much Testing is Enough?

May Depend on:

- Risk Assessment
- Level of Configuration
- Complexity of System
- Criticality of System
- Number of Connections w/ Other Systems and Equipment
- Level of Prior System Validation, Experience, Knowledge
- Impact of the System on the Process/Product
- Span of System Control Over Facility/Process/Product
- Level of Control of Operators Over System
- Transparency of Computer System Decisions

Applicable Regulations

- 21 CFR Part 11: Electronic Records; Electronic Signatures
- 21 CFR Section 211.68: Automatic, Mechanical, and Electronic Equipment
- 21 CFR Sections 820.70(i) and 820.72: Quality System Regulations
- 21 CFR Section 1271.160(d): Computers

Revisions to CGMP Regulations

Final Rule: Federal Register Notice, Vol. 73, No. 174, pp.51919-51933 to modify 21 CFR 211.68: Automatic, Mechanical, and Electronic Equipment

New paragraph 211.68(c): Such automated equipment used for performance of operations addressed by § 211.101(c) or (d), 211.103, 211.182, or 211.188(b)(11) can satisfy the requirements included in those sections relating to the performance of an operation by one person and checking by another person if such equipment is used in conformity with this section, and one person checks that the equipment properly performed the operation.

Changes were also made accordingly to each individually cited regulation noted above.

Part 11: Current Thinking (1)

As described below, the approach outlined in the August 2003 Part 11 Guidance for Industry is based on three main elements:

- Part 11 will be interpreted narrowly
- We intend to exercise enforcement discretion with regard to Part 11 requirements for validation, audit trails, record retention, and record copying in the manner described in this guidance and with regard to all Part 11 requirements for systems that were operational before the effective date of Part 11 (also known as legacy systems).
- We will enforce all predicate* rule requirements, including predicate rule record and recordkeeping requirements.

*

The underlying requirements set forth in the Act, PHS Act, and FDA regulations, other than Part 11 (e.g. 21 CFR 211, 600s, 800s, 1270s, etc.).

Part 11: Current Thinking (2)

- Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations.
- That is, we do not intend to take enforcement action to enforce compliance with the validation, audit trail, record retention, and record copying requirements of part 11 as explained in this guidance.
- However, records must still be maintained

Part 11: Current Thinking (3)

We intend to enforce provisions related to the following controls and requirements:

- Limiting System Access to Authorized Individuals
- Use of Operational System Checks
- Use of Authority Checks
- Use of Device Checks
- ..Persons Who...Use Electronic Systems Have the Education, Training, and Experience...
- ...Written Policies That Hold Individuals Accountable

Guidance: Software Validation (1)

*General Principles of Software Validation;
Final Guidance for Industry and FDA Staff:
January 11, 2002*

- Defined User Requirements
- Validation of Off-the-Shelf Software
- Traceability Analysis
- Defect Prevention
- Software risk analysis

Guidance: Software Validation (2)

General Principles... (Cont.)

Quality Planning:

- Methods/Procedures
- Acceptance Criteria
- Inputs/Outputs
- Roles and Responsibilities
- Risks and Assumptions
- Documentation

Guidance: Software Validation (3)

General Principles... (Cont.)

- Level of Structural Testing or “Coverage”
- Error Handling
- Ranges, Limits and Defaults
- Control Logic, Data Structures, Data Flow Diagrams
- Security Measures (Physical and Logical)

Submission Content (1)

Major Computer Systems that Control/Monitor the Process:

- List of Steps Controlled/Monitored
- List of Parameters Monitored
- Alerts and Alarms
- Equipment or Human/Machine Interfaces
- Certification that IQ and OQ are Complete
- Procedures for Making Changes to the System

Submission Content (2)

- Validation Data Summary
- Data Collection and Management
- Process Validation Lots (Depending Upon the Change)
- System Configuration
- Software Testing
- Validation Issues and Deviations

Inspection Coverage (1)

All documents related to computer system, including:

- User Requirements
- Design Specifications
- Software Configuration
- Systems Integration
- Data Generated by System

Inspection Coverage (2)

All documents related to computer system, including:

- Test Cases
- User Acceptance Testing
- Configuration Management (Change Control)
- Batch Records
- Investigations/Deviations
- Log Books
- Live System Demonstration

Inspection Example

DCS System for Some Unit Operations (purification, concentration, CIP):

- Validation of DCS system early in product development
- Process changed over time
- Upgrade of system (hardware and software upgrades, but no major change in functionality)
- Batch record: Information captured on paper and electronically
- During inspection, comparison of paper batch records and DCS recipe revealed two divergent processes – paper vs. electronic
- Two sets of process limits were completely different – Firm relied on paper-based limits
- Much wider tolerances for DCS system (alarms were never triggered, even when outside the process limits as defined by the batch record)

Type C Meetings

Possible Discussion Topics:

- Major Computer Systems to be Used in Your New or Upgraded Facility
- Validation Plans for the Systems
- CBER Expectations

Special Thanks To:

- Mary A. Malarkey, CBER
- John A. Eltermann, Jr., R.Ph., M.S., CBER
- Laurie Norwood, MS, CBER
- Chiang Syin, PhD, CBER