IVT's 16th Annual Computer and Software Validation

Ensuring Data Integrity

Joseph Zec
Associate Director, Technology Quality Management
PAREXEL International
April 28, 2015

Agenda

Data integrity is a shared goal between industry and regulators!

- Regulatory perspective
- Data integrity during system development and validation
- Data integrity during production use
- Interactive exercise – data integrity concerns for a computerized CAPA system

Discussion

Word Association

- What does “data integrity” mean to you?

Data integrity is a shared goal between industry and regulators

Data integrity is not just a compliance issue

- Data integrity issues could lead to patient safety concerns
- Data integrity issues could lead to business operations concerns
- In many ways, industry has more of an invested interest in data integrity than regulators!

Regulations and Data Integrity

- Data recorded on paper – GDP
- Data recorded electronically – 21 CFR Part 11 / EU Annex 11
- Part 11 Preambles
- Part 11 Guidance
  - Scope and Application
  - Computerized Systems in Clinical Investigations

Regulations and Data Integrity

What it all boils down to:

- Removal of ambiguity
- Removal of lack of attribution

21 CFR Part 11

11.1 Scope:

"Electronic records and signatures…to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."

21 CFR Part 11

11.1 Scope:

Part 11 applies to:

- Records & signatures required by predicate rules
  - This includes any records defined as part of an organization's Quality System (21 CFR Part 820)
- Records submitted to the agency

21 CFR Part 11

11.10 Controls for closed systems:

"Persons who used closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure the signer cannot readily repudiate the signed record as not genuine."

21 CFR Part 11 / EU Annex 11

11.10 Controls for closed systems:

- Validate systems (EU Annex 11: System (7))
- Generate accurate and complete copies of records (EU Annex 11: System (12))
- Protect records (EU Annex 11: System (13, 14))
- Limit system access (EU Annex 11: System (8))
- Employ audit trails (EU Annex 11: System (10))

21 CFR Part 11

11.50 Signature manifestations:

Signature integrity encompasses:

- Printed name
- Date and time
- Meaning of signature

21 CFR Part 11

Subpart C – Electronic Signatures:

Signature integrity also encompasses:

- Uniqueness to an individual
- Use of 2 identification components
- Only 1 component required "during a single, continuous period of controlled system access"
- Fraudulent use "requires collaboration of two or more individuals"

21 CFR Part 11

11.70 Signature/record linking:

Signatures must be linked to their respective records such that the signatures "cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means."

21 CFR Part 11

11.300 Controls for 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."

21 CFR Part 11

11.300 Controls for identification codes/passwords:

- Uniqueness
  - Retirement of electronic signature components
- Maintenance
- Loss management procedures
- "Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use…"

Discussion

From the Part 11 Preambles:

In FDA's view, the significance of such attempts requires the immediate and urgent attention of appropriate security personnel in the same manner that individuals would respond to a fire alarm.

How has your organization dealt with the "immediate and urgent manner" provision of Part 11?

Part 11 Preambles

Comment: Systems in place prior to the release of Part 11 should be grandfathered

FDA response: Since these systems are currently used to generate electronic regulatory records, they still pose integrity concerns

Part 11 Preambles

Comment: Part 11 controls should only start when a record is accepted by an organization

FDA response: This could lead to compromised records since the need for integrity starts when the record is first created

Part 11 Preambles

From the Preambles Introduction:

"Reducing the likelihood that someone can readily repudiate an electronic signature as not his or her own, or that the signed record has been altered, is vital to the agency's basic acceptance of electronic signatures."

Part 11 Preambles

Comment: Time should only be recorded in audit trail when feasible

FDA response: Time is critical in documenting a sequence of events on a given day

Part 11 Preambles

Comment: Requirements for electronic record/electronic signature linking are too prescriptive, unnecessary, unattainable, and excessive

FDA response: "A technology based link is necessary" vs. procedural or administrative controls. "Record falsification" is the concern here

Part 11 Guidance

February 2003 – FDA withdraws all existing Part 11 guidance and announces enforcement discretion for the following areas:

- Validation
- Audit trail
- Record retention
- Record copying

Part 11 Guidance – Scope & Application

Many data integrity related Part 11 controls and requirements were left untouched:

- Limit system access to authorized individuals
- Operational system checks
- Authority checks
- All E-signature requirements

Part 11 Guidance – Computerized Systems in Clinical Investigations

Section I:

"…this guidance is intended to assist in ensuring confidence in the reliability, quality, and integrity of electronic source data and source documentation (i.e. electronic records)"

Part 11 Guidance – Computerized Systems in Clinical Investigations

Section II – "Quality" data (integrity):

- Attributable
- Legible
- Contemporaneous
- Original
- Accurate

Part 11 Guidance – Computerized Systems in Clinical Investigations

Section IV-B:

Guidance from this section includes:

- Limiting system access
- Use of audit trails
- Use of date/time stamps
  - Correct system date and time
  - Unambiguous
  - Identification of time zones

Part 11 Guidance – Computerized Systems in Clinical Investigations

Section IV-F-1 – data entry:

- System design should promote accurate data entry
- Beware of auto-population of data fields (default values)

Data Integrity – System Development & Validation

Data integrity starts with requirements!

- Security requirements
  - Individual login codes and passwords
  - Periodic password maintenance
  - Authority checks
  - Permission matrices
  - Physical requirements

Data Integrity – System Development & Validation

- Data loss protection requirements
  - Back-up requirements
  - Restore requirements
  - Disaster recovery requirements
  - Physical requirements

Data Integrity – System Development & Validation

- Audit trail requirements
  - What was changed?
  - What was the original value?
  - What was the value changed to?
  - Who changed it?
  - When was it changed?
  - Where was it changed?
  - Why was it changed?

Data Integrity – System Development & Validation

- Data correctness requirements
  - Enforce process workflow where possible
  - Perform input checks
    - Data entered by users
    - Data entered automatically through integrations with other systems

Data Integrity – System Development & Validation

- E-signature requirements
  - Uniqueness
  - Two identification components (unless biometrics are being used)
  - Used only by owner
  - Falsification deterrents
  - Periodic maintenance
  - Loss management

Data Integrity – System Development & Validation

Data integrity concerns are identified via risk assessment

- Assess each requirement (and the system as a whole) for data integrity concerns
  - Not all requirements are created equally in terms of data integrity risks
  - Create a ranking system (high, medium, low) that identifies those requirements that, should the system fail to meet them for any reason (failure mode), a data integrity issue could result
  - These requirements can now be more robustly designed and validated

Data Integrity – System Development & Validation

Data integrity is implemented and enhanced by system design

- A clever design can reduce the likelihood of data integrity issues arising during production use
  - Design a robust backup/restore/disaster recovery process
  - Implement tight access controls
  - Implement a robust audit trail
  - Design unambiguous e-signature mechanisms
  - Create rigid e-signature-document linkages
  - Implement data entry prompts/help text/input checks

Data Integrity – System Development & Validation

Data integrity is verified by various verification techniques:

- Analysis
  - Risk
  - Traceability
  - Configuration
- Review
  - Requirements
  - Design
  - Source code
  - Test scripts
  - Procedures
  - Training material

Data Integrity – System Development & Validation

Data integrity is verified by various verification techniques:

- Testing
  - Unit / Integration
  - Installation
  - System / User acceptance
- Requirements with high data integrity risk deserve robust testing
  - Performance / Stress
  - Negative / Error
  - Boundary / Limits
- Do not fail to test backup/restore/disaster recovery procedures!

Data Integrity – Production Use

Data integrity is maintained through procedures, training, and vigilance:

- Detailed system use & maintenance procedures with data integrity discipline built-in
- Strict, verified adherence to procedures
- Regular training for applicable personnel focusing on data integrity topics

Data Integrity – Interactive Exercise

Let's pretend we're building our own CAPA system. We'll need to identify and deal with data integrity issues at various levels – risk assessment, requirements, design, and testing.

The group will break into 4 teams to examine one each of these levels, and use the worksheets to guide them in documenting their discussions.

Data Integrity – Worksheet Example

Data Integrity Worksheet – CAPA System **Requirements** – List of Data Integrity Concerns

Area	**Concerns and how to address them**
Record protection	Loss of CAPA files – include requirements for backup/restore/disaster recovery
Limit access to data	
Use audit trails	
Enforce workflow	
Check authority	
Check input	
E-signatures	
Other	