DIGITAL QUALITY ASSOCIATES
WHERE EXPERIENCE COUNTS

# Part 2: The Evolution of IT Quality and Validation in Clinical Trials: Understanding ICH E6(R3) GCP Guidelines and Related Regulations

## Data Integrity and Security

### ICH E6(R3) Requirements

Data integrity and security requirements are extensively covered throughout ICH E6(R3), particularly in sections 4.3.3. The guideline emphasizes that "The security of the trial data and records should be managed throughout the data life cycle" (section 4.3.3(a)).

Key requirements include:

1. System Security Controls: "The responsible party should ensure that security controls are implemented and maintained for computerised systems. These controls should include user management and ongoing measures to prevent, detect and/or mitigate security breaches. Aspects such as user authentication requirements and password management, firewall settings, antivirus software, security patching, system monitoring and penetration testing should be considered" (section 4.3.3(b)).

2. Data Backup: "The responsible party should maintain adequate backup of the data" (section 4.3.3(c)).

3. Disaster Recovery: "Procedures should cover the following: system security measures, data backup and disaster recovery to ensure that unauthorised access and data loss are prevented. Such measures should be periodically tested, as appropriate" (section 4.3.3(d)).

4. Protection from Unauthorized Access: "The sponsor should ensure that trial data are protected from unauthorised access, disclosure, dissemination or alteration and from inappropriate destruction or accidental loss" (section 3.16.1(v)).

5. Incident Reporting: "The sponsor should have processes and procedures in place for reporting to relevant parties, including regulatory authorities, incidents (including security breaches) that have a significant impact on the trial data" (section 3.16.1(w)).

## Relationship to GDPR and Other Data Protection Regulations

ICH E6(R3) complements but does not replace the requirements of data protection regulations such as:

1. General Data Protection Regulation (GDPR): For trials conducted in the EU or involving EU residents, GDPR requirements for personal data protection must be followed alongside ICH E6(R3).

2. Health Insurance Portability and Accountability Act (HIPAA): US trials must comply with HIPAA Privacy and Security Rules in addition to ICH requirements.

3. Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and similar laws in other countries.

ICH E6(R3) acknowledges these overlapping requirements, stating that "The investigator/institution should implement appropriate measures to protect the privacy and confidentiality of personal information of trial participants in accordance with applicable regulatory requirements on personal data protection" (section 2.12.7) and that "The sponsor should implement appropriate measures to protect the privacy and confidentiality of personal information of trial participants, in accordance with applicable regulatory requirements on personal data protection" (section 3.16.1(t)).

## Practical Implementation

Organizations should consider implementing:

1. A comprehensive information security management system that addresses clinical trial-specific requirements

2. Regular security risk assessments of clinical trial systems

3. Encryption of sensitive data both in transit and at rest

4. Role-based access controls for all clinical trial systems

5. Security incident response procedures specific to clinical trial data

6. Regular security awareness training for all staff involved in clinical trials

## Data Life Cycle Management

### ICH E6(R3) Framework

Section 4.2 of ICH E6(R3) provides a comprehensive framework for data life cycle management in clinical trials. The guideline states that "Procedures should be in place to cover the full data life cycle" and outlines key elements including:

1. Data Capture: "When data captured on paper or in an electronic health record are manually transcribed into a computerised system (e.g., data acquisition tool), the need for and the extent of data verification should take the criticality of the data into account" (section 4.2.1(a)).

2. Metadata Management: The guideline requires evaluating systems to ensure "Systems are designed to permit data changes in such a way that the initial data entry and any subsequent changes or deletions are documented, including, where appropriate, the reason for the change" (section 4.2.2(a)(ii)).

3. Audit Trails: Section 4.2.2(b) specifies that "Audit trails should not be modified except in rare circumstances (e.g., when a participant's personal information is inadvertently included in the data) and only if a log of such action and justification is maintained."

4. Data Review: "Procedures for review of trial-specific data, audit trails and other relevant metadata should be in place. It should be a planned activity, and the extent and nature should be risk-based, adapted to the individual trial and adjusted based on experience during the trial" (section 4.2.3).

5. Data Corrections: "There should be processes to correct data errors that could impact the reliability of the trial results. Corrections should be attributed to the person or computerised system making the correction, justified and supported by source records around the time of original entry and performed in a timely manner" (section 4.2.4).

6. Data Transfer and Migration: "Validated processes and/or other appropriate processes such as reconciliation should be in place to ensure that electronic data, including relevant metadata, transferred between computerised systems retains its integrity and preserves its confidentiality" (section 4.2.5).

7. Data Finalization: "Data of sufficient quality for interim and final analysis should be defined and are achieved by implementing timely and reliable processes for data capture, verification, validation, review and rectification of errors and, where possible, omissions that have a meaningful impact on the safety of trial participants and/or the reliability of the trial results" (section 4.2.6(a)).

8. Data Retention and Destruction: Section 4.2.7 requires that "The trial data and relevant metadata should be archived in a way that allows for their retrieval and readability and should be protected from unauthorised access and alterations throughout the retention period." Section 4.2.8 states that "The trial data and metadata may be permanently destroyed when no longer required as determined by applicable regulatory requirements."

## Connection to ALCOA+ Principles

ICH E6(R3) requirements align closely with the widely recognized ALCOA+ principles for data integrity, which include:

- Attributable: Data should be attributable to the person who generated it. ICH E6(R3) requires that "Corrections should be attributed to the person or computerised system making the correction" (section 4.2.4).
- Legible: Data should be readable and permanent. ICH E6(R3) requires that audit trails and logs be "interpretable and can support review" (section 4.2.2(c)).
- Contemporaneous: Data should be recorded at the time of the activity. Section 4.2.2(d) requires "the automatic capture of date and time of data entries or transfer are unambiguous."
- Original: Original data or a certified copy should be maintained. Section 2.12.2 requires that "Source records should be attributable, legible, contemporaneous, original, accurate and complete."

- Accurate: Data should be correct, complete, and truthful. ICH E6(R3) requires processes to correct data errors that could impact reliability (section 4.2.4).
- Complete: All data, including metadata, should be complete. Section 4.2.1(b) requires that "Acquired data from any source should be accompanied by relevant metadata."

While ICH E6(R3) does not explicitly reference ALCOA+, its requirements for audit trails, data corrections, and metadata management clearly reflect these principles

### Relationship to Other Data Management Guidelines

The data lifecycle provisions in ICH E6(R3) should be considered alongside:

1. CDISC Standards: Clinical Data Interchange Standards Consortium (CDISC) provides standards for data structure and exchange that complement the ICH E6(R3) data lifecycle requirements.

2. ICH E9(R1): This addendum on estimands and sensitivity analysis has implications for how data are collected, managed, and analysed throughout the data lifecycle.

3. FDA Data Standards Catalog: For submissions to the FDA, this catalog specifies required data standards.

4. EMA Guidance on Data Management: The European Medicines Agency provides additional guidance on clinical data management practices.

## User Management and Training

### ICH E6(R3) User Management Requirements

Section 4.3.8 of ICH E6(R3) outlines specific requirements for user management in clinical trial systems:

1. Access Controls: "Access controls are integral to computerised systems used in clinical trials to limit system access to authorised users and to ensure attributability to an individual. The security measures should be selected in such a way that they achieve the intended security" (section 4.3.8(a)).

2. Role-Based Access: "Procedures should be in place to ensure that user access permissions are appropriately assigned based on a user's duties and functions, blinding arrangements and the organisation to which users belong. Access permissions should be revoked when they are no longer needed. A process should be in place to ensure that user access and assigned roles and permissions are periodically reviewed, where relevant" (section 4.3.8(b)).

3. Access Documentation: "Authorised users and access permissions should be clearly documented, maintained and retained. These records should include any updates to a user's roles, access permissions and time of access permission being granted (e.g., time stamp)" (section 4.3.8(c)).

4. Investigator Access Oversight: The sponsor must "ensure that access permissions granted to investigator site staff are in accordance with delegations by the investigator and visible to the investigator" (section 3.16.1(x)(iv)).

The guideline also addresses training requirements, stating that "The responsible party should ensure that those using computerised systems are appropriately trained in their use" (section 4.3.2).

## Integration with Delegation of Authority Requirements

These user management requirements should be viewed in conjunction with the broader delegation of authority framework outlined in sections 2.3 (Investigator Responsibilities) and 3.3 (Sponsor Allocation of Activities). The guideline states that "The investigator may delegate trial-related activities to other persons or parties" (section 2.3.1) but "retains the ultimate responsibility and should maintain appropriate oversight of the persons or parties undertaking the activities delegated to ensure the rights, safety and well-being of the trial participants and the reliability of data" (section 2.3.1).

This has important implications for user management, as system access rights should align with the documented delegation of trial-related activities. This connection between delegation logs and system access controls represents a key area for sponsor and investigator oversight.

## Training Documentation Requirements

While ICH E6(R3) specifies that users should be appropriately trained, it also includes broader training documentation requirements:

1. "The investigator should ensure that persons or parties to whom the investigator has delegated trial-related are appropriately qualified and are adequately informed about relevant aspects of the protocol, the investigational product(s) and their assigned trial activities" (section 2.3.2).

2. "Trial-related training to persons assisting in the trial should correspond to what is necessary to enable them to fulfil their delegated trial activities that go beyond their usual training and experience" (section 2.3.2).

3. "Trial-specific training records" are identified as potential essential records (C.3.2 Essential Records Table).

These requirements highlight the need for a comprehensive training program that encompasses not only system use but also the broader protocol and regulatory requirements relevant to delegated tasks.

# System Failure and Technical Support

## System Failure Management

ICH E6(R3) explicitly addresses system failure in section 4.3.6, stating: "Contingency procedures should be in place to prevent loss or lack of accessibility to data essential to participant safety, trial decisions or trial outcomes."

This requirement emphasizes the need for business continuity planning specific to clinical trial systems, particularly those that manage critical data related to participant safety and trial outcomes.

Organizations should implement:

1. System redundancy for critical applications

2. Regular backup testing procedures

3. Documented recovery processes with defined recovery time objectives

4. Regular training on contingency procedures

## Technical Support Requirements

Section 4.3.7 outlines requirements for technical support, including:

1. Issue Management: "Where appropriate, there should be mechanisms (e.g., help desk support) in place to document, evaluate and manage issues with the computerised systems (e.g., raised by users), and there should be periodic review of these cumulative issues to identify those that are repeated and/or systemic" (section 4.3.7(a)).

2. Prioritized Resolution: "Defects and issues should be resolved according to their criticality. Issues with high criticality should be resolved in a timely manner" (section 4.3.7(b)).

These requirements highlight the importance of having structured technical support processes that not only address immediate system issues but also facilitate continuous improvement through regular review of cumulative issues.

## Essential Records for Clinical Trials

ICH E6(R3) provides comprehensive guidance on essential records in Appendix C, which is particularly relevant to IT and validation documentation. The guideline states that essential records are "the documents and data (and relevant metadata), in any format, associated with a clinical trial that facilitate the ongoing management of the trial and collectively allow the evaluation of the methods used, the factors affecting a trial and the actions taken during the trial conduct to determine the reliability of the trial results" (Glossary).

Several types of IT-related records are specifically identified as essential in Table 2 of Appendix C, including:

1. "Documentation of trial-specific computerised system validation (e.g., specifications, testing, validation report, change control)"

2. "Documentation of the assessment of fitness for purpose for non-trial-specific computerised systems used in the trial (e.g., clinical practice computerised systems)"

3. "Instructions for use of important trial-specific systems (e.g., interactive response technologies (IRTs) user manual, electronic CRF (eCRF) manual)"

4. "Records demonstrating fitness for purpose (e.g., maintenance and calibration) for equipment used for important trial activities"

These requirements underscore the importance of maintaining comprehensive documentation of system validation, assessment, and use throughout the clinical trial lifecycle.

**Look out for Part 3**

**Coming soon**