



Module 3.3b Transcript

Interpretation and Application of ICH E6(R3):

GOOD CLINICAL PRACTICE (GCP)

Welcome back to the Interpretation and Application of ICH E6(R3): Good Clinical Practice.

Module 3 of this training discusses Data Governance in clinical trials.

Module 3 contains 4 sub-modules, which should be taken sequentially. This is Module 3.3b.

In this module, we'll continue to answer:

- How should a risk-proportionate approach be applied to managing computerised systems in a clinical trial? And,
- What are the responsibilities of sponsors and investigators for managing computerised systems?

Determining whether a computerised system is fit for purpose depends on many factors. This includes the extent to which the requirements in section 4.3 and the metadata requirements in section 4.2 are addressed proportionately throughout the system lifecycle. A system that is fit for purpose helps ensure that investigator and sponsor responsibilities, outlined in sections 2.12.10(c) and 3.16.1(x) are met.

These requirements include managing the system's metadata and validating the system correctly. They also cover system security and user management. Additionally, section 4.3 highlights the importance of timely system releases, managing system failures, providing adequate technical support, implementing proper procedures, training end users, and periodic review of these requirements throughout the system lifecycle.

In this module, we will examine each of these specific requirements for computerised systems and discuss how a fit for purpose assessment informs their design and implementation, as well as the respective responsibilities of sponsors and investigators in managing these requirements.

Sub-module 3.3b aims to address the importance of these factors in the context of the Crohn's Disease case. The intention is not to address each specific requirement in section 4.3 of the guideline but to focus on selected requirements relevant to the case.

For each of the requirements we will:

- Identify a potential risk of importance to the Crohn's Disease case, and
- Propose risk mitigations and thereby address selected requirements.

We'll begin with the system's metadata.

Click on "Metadata" to continue.

Section 4.2.1(b) states that “acquired data from any source, including data directly captured in a computerised system should be accompanied by relevant metadata.”

Metadata is defined in the E6(R3) glossary as “the contextual information required to understand a given data element. Metadata is structured information that describes, explains or otherwise makes it easier to retrieve, use or manage data.”

For the purposes of the E6(R3) guideline, “relevant metadata” are defined as those needed to allow the appropriate evaluation of trial conduct.

To that end, in the Crohn’s Disease case example, it is important that the eCOA system captures relevant metadata, including the date and time of data capture, the ID of the device used, the participant number of the participant entering data, user roles and permission logs, and audit trails.

The device should also capture audit trails, an important type of metadata.

Audit trails are defined in the E6(R3) glossary as “metadata records that allow the appropriate evaluation of the course of events by capturing details on actions (manual or automated) performed relating to information and data collection and, where applicable, to activities in computerised systems.”

The definition goes on to state that the audit trail should “show activities, initial entry and changes to data fields or records, by whom, when and, where applicable, why. In computerised systems, the audit trail should be secure, computer-generated and time stamped.”

Now, let’s apply the guideline thinking using examples from the Crohn’s Disease case. In this context, we can clearly see how different systems come into play.

Click on the eCOA system to continue.

In Module 3.2, we identified the eCOA system as critical to quality because it handles co-primary endpoint data.

And, in Module 3.3a, we saw that the eCOA system is an example of a system deployed by the sponsor for clinical trial purposes.

One potential risk to the eCOA system is inadequate audit trails that do not permit data capture and changes in such a way that is traceable.

The capture of (and changes to) primary efficacy endpoint data should be fully traceable and transparent across the entire data lifecycle, from initial capture, through review and analysis, and ultimately to reporting.

If it is not possible to determine who entered or changed the data, what was changed, when, or why, confidence in the data is diminished and regulators may be

unable to rely on it. In addition, appropriate audit trails allow the investigators to confirm that participants at their site are entering data as required by the protocol.

As part of the fit for purpose assessment for the eCOA system, the sponsor should evaluate the system for the types and content of metadata available to ensure that:

- The system is 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
- The system records and maintains workflow actions in addition to recording and maintaining direct data entry and data changes in the system
- System audit trails and logs are interpretable and can support review, and
- The automatic capture of date and time of data entries or transfer are unambiguous

Next, we'll look at validation. Click "validation" to continue.

Systems should be validated as fit for purpose prior to use in the trial, including those developed by service providers.

Validation should demonstrate that the system conforms to the established requirements for completeness, accuracy and reliability and that its performance is consistent with its intended purpose.

The approach to validation should be based on a risk assessment that considers:

- the intended use of the system
- the purpose and importance of the data and records that are generated, maintained and retained in the system, and
- the potential of the system to affect the rights, safety, and wellbeing of trial participants and the reliability of trial results.

We have identified the eCRF used in the Crohn's Disease case as a sponsor-deployed system that was designed for clinical trial purposes. We also identified it as a system that is critical to quality in this trial because it maintains co-primary efficacy endpoint data.

This is a commercial system developed by a service provider that is configured according to the protocol for use in the trial. Additionally, a custom, trial-specific functionality has been built into the eCRF, enabling automatic calculation of the CDAI score based on data from participants and clinicians and laboratory data.

All three CDAI-related data flows include a step where the eCRF automatically calculates the CDAI score from the data entered. Because this score is used to assess disease activity and supports the co-primary efficacy endpoints and key trial decisions, it is essential that the eCRF performs this calculation correctly. Special

attention and oversight should therefore be given to validating and monitoring this eCRF functionality to ensure the accuracy and reliability of the CDAI scores.

Two potential risks related to the eCRF include:

- Programming errors resulting in calculation errors of the CDAI score, and
- Incorrect configuration and poorly designed eCRF screens so that entry fields, questions, response options, and instructions are not easy to understand

This is important because these risks can lead to incorrect scores and data entry errors in the fields used for CDAI score calculation (e.g., the fields used to capture haematocrit values).

These errors would directly impact the trial results. To avoid this, appropriate validation of this key functionality is essential.

Risk mitigation strategies that could be taken by the sponsor include:

- Defining the requirements and specifications for the system, along with plans for testing them
- Conducting validation testing of key system functions to ensure they work as intended, for example, testing that the CDAI calculations produce correct outputs, and that edit checks are in place to prevent incomplete, inconsistent, or illogical data entries such as ensuring that data entry fields are designed to accept the appropriate format and range of values.
- Performing validation testing of important interfaces between systems to confirm that they communicate and function correctly together, and
- Carrying out user acceptance testing to validate that the system meets requirements and works as expected for end users.

Further risk mitigation strategies might include:

- Implementing change control and performing re-validation, as applicable based on risk, to ensure that errors are not introduced later in the system lifecycle, considering both previously collected and new data
- Implementing procedures for system design, system requirement, functionality testing, configuration, release, setup, installation and change control, and
- Maintaining and retaining validation documentation.

The next requirement we'll address is IT security. Click "Security" to continue.

There is a risk to the reliability of trial data and the protection of personal data if security controls are insufficient to prevent, detect, and respond to security incidents.

For example, in the Crohn's Disease case, a vulnerability in the trial system could lead to a malware or ransomware attack affecting the eCRF used in the trial.

An incident like this could temporarily—or even for a longer period—block access to the eCRF. It could also lead to trial data being exposed, encrypted, corrupted, or even lost, including sensitive information.

As a result, the integrity and availability of key endpoint and safety data could be affected. Safety reporting—especially for serious adverse events—might be delayed, and day-to-day trial activities like data entry and patient enrolment could be disrupted.

Because trial data and records should be kept secure throughout the trial, the sponsor should ensure that appropriate security controls are implemented and maintained, including user management controls and risk-based measures to prevent, detect and/or mitigate security breaches, such as user authentication, password management, firewalls, antivirus software, security patching, system monitoring and penetration testing.

The sponsor should also ensure that procedures for system security, data backup and disaster recovery are implemented and maintained to ensure that unauthorised access and data loss are prevented and that security, backup and disaster recovery measures are periodically tested, as appropriate.

To continue, click “User management.”

User management and access controls are essential to limit system access to authorised users and to ensure attributability to an individual.

In Module 3.2, we identified that safeguarding blinding is a key process in clinical trials. Because the Crohn’s Disease case example is a double-blinded trial, maintaining the integrity of the blinding is a critical to quality factor.

A potential risk to this critical to quality factor is inappropriate access to unblinded information. If user management and access controls are inadequate, staff who should remain blinded may inadvertently see treatment assignments or other sensitive information. For example, a blinded statistician making key decisions – such as defining analysis populations – could be influenced by knowledge of the treatments, even unknowingly.

Such bias could compromise the reliability and validity of trial results.

Therefore, in blinded clinical trials it is important to address this risk and ensure that the right people are given the right access permissions to maintain the integrity of the blinding and also to protect the confidentiality of participants’ information and data.

To mitigate this risk, the sponsor should:

- Select access controls in such a way that they achieve the intended security

- Implement procedures to ensure that user access permissions are appropriately assigned based on a user's duties and functions in a trial, blinding arrangements described in the protocol, and the organisation to which users belong
- Revoke access permissions when they are no longer needed and ensure that user access and assigned roles and permissions are periodically reviewed, where relevant, and
- Document, maintain and retain records on authorised users and access permissions.

Next, we'll look at system release. Click to continue.

For the Crohn's Disease case, a potential risk to data reliability exists if the eCOA system and the eCRF are not ready for use prior to their required use in the trial or if they are released prior to appropriate validation.

This is important because if a system is released before fully validated, it might contain errors, such as mistakes in the CDAI calculation function. It could also be released without implemented edit checks. Further, if the system isn't ready when the trial begins, investigator sites may need to use temporary alternative data collection processes until the system is ready.

This can pose unnecessary burden and uncertainty to sites and participants as they will need to be instructed in several different data collection methods and will potentially have to retrospectively address queries from late edit checks.

Further, there is a risk of late detection of problems with data entry, because data and metadata cannot be reviewed in a timely manner unless mitigating actions are implemented.

Strategies that could be taken to mitigate these risks include:

- Ensuring that systems, including both standard functionality, trial specific functionality and interfaces, are only released after appropriate validation, and
- Resolving or appropriately mitigating identified issues prior to release.

Trial-specific systems should only be implemented, released or activated for individual investigator sites after all necessary approvals for the clinical trial relevant to that investigator site have been received.

This applies not only at the time of initial system release but also for release of system updates, particularly for changes made as a result of a protocol amendment.

Next, we'll look at system failure and technical support together. Click to continue.

Returning to the Crohn's Disease case, let's look at the risk of system outages, device malfunction, or synchronisation failures for the eCOA system, including the eDiaries

used by participants, which has previously been identified as a system of higher criticality in this trial.

A potential risk to data reliability exists if the operation of the eCOA system fails, for example if there are connectivity issues or other problems accessing the eDiary application.

The risk involves losing primary endpoint data from participants, which is particularly severe because the data are captured directly on the device and cannot be reconstructed from any other source.

To mitigate this risk of data loss, the sponsor should:

- Implement contingency procedures to prevent loss or lack of accessibility to data essential to participant safety, trial decisions or trial outcomes
- Have mechanisms such as help desk support in place to document, evaluate and manage issues with the computerised systems (e.g., issues raised by users)
- Review such issues to identify those that are repeated and/or systemic, and
- Resolve defects and issues in a timely manner according to their criticality.

Next, we'll look at the importance of documented procedures and appropriate training in the use of computerised systems. Click to continue.

Let's return once again to the eCOA system used in the Crohn's Disease case. It is critical to quality that participants and the investigator site staff use the system as intended, for example that they know how to sign in, enter data, and what to do if the user forgets their password.

A potential risk to data reliability exists if the eCOA system is not used as intended, for example, if participants do not enter data correctly due to misunderstandings or lack of training.

The risk involves having erroneous primary endpoint data entered by participants, which could impact trial results. As the data are captured directly on the device and cannot be reconstructed from any other source, appropriate participant understanding and use of the system is particularly crucial.

Risk mitigation strategies include:

- Implementing procedures to ensure their appropriate use in clinical trials for essential activities related to data collection, handling and management
- And ensuring that those using computerised systems are appropriately trained in their use.

This training should be directed to the needs of the users and how critical their system-related tasks are to the trial.

The final requirement we'll address is periodic review. Click to continue.

Measures put in place to protect data integrity should be checked periodically to ensure they still work as intended.

How often and how rigorously these checks are done should depend on how critical the system is to the trial, and how important the data are for protecting trial participants and ensuring the reliability of trial results. This includes periodic testing to ensure:

- The validated state of a system
- The user accesses of a system and assigned roles and permissions, and
- The security settings of a system

Further, any issues identified through technical support should be periodically reviewed to identify any recurring or systemic problems. These issues should be addressed according to their criticality, with high-criticality issues resolved in a timely manner.

This periodic testing or review should be clearly documented.

For example, in the Crohn's Disease case, it is essential to resolve connectivity or other technical issues for the participant in a timely manner to prevent loss of data.

In summary, sponsors and investigators responsible for overseeing and managing computerised systems should adopt a risk-based approach, ensuring that the level of oversight and risk mitigation measures implemented are proportionate to the system's criticality and its potential impact on participant protection and trial results.

Thank you for completing Module 3.3b. Next, we'll finish the data governance module by looking at data lifecycle management.