

Module 3.2 Transcript

Interpretation and Application of ICH E6(R3):

GOOD CLINICAL PRACTICE (GCP)

Welcome 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 3.2: Risk-Proportionate Approach to Data Governance.

Key questions you will be able to answer after completing this module include:

- How does the concept of risk proportionality apply to data governance?
- What are the key steps in implementing a risk-based approach to data governance? And,
- How can mapping and analysing data flows help identify critical to quality factors?

Many of the GCP principles of the E6(R3) guideline support taking a risk-proportionate approach to trial design and conduct, including data governance activities.

In particular, Principles 9.2, 9.3, and 9.4 provide a solid foundation for developing risk-based data governance strategies by emphasising fit for purpose approaches to the design of systems and processes. These principles also highlight the central role of critical to quality factors in guiding data governance activities and decisions.

Section 4 of the E6(R3) guideline states that systems and processes that help ensure clinical trial quality should be designed and implemented in a way that is proportionate to the risks to participant protection and the reliability of trial results.

This means that not all data, systems, and processes require the same level of management and oversight. Rather, the level of management and oversight should be based on the criticality of the data, systems, and processes and be proportionate to the risks to participant protection and the reliability of the trial results.

The evaluation of data criticality is a fundamental component of the risk assessment process and is central to the Quality by Design and Quality Management approach. Within this risk-based framework, data criticality is assessed based on the data's potential impact on trial participants' rights, safety, and well-being, as well as on the reliability and interpretability of trial results.

Importantly, data criticality should not be viewed as a binary classification, meaning data should not be viewed as simply "critical" or "not critical".

Rather, data criticality exists along a continuum. Clinical trial data may carry varying degrees of importance depending on their context, use, and potential consequences if inaccurate, incomplete, or missing.

For example, in the Crohn's Disease case example introduced in Module 3.1, data related to co-primary efficacy endpoints should be considered data of higher

criticality on this continuum. Data of higher criticality would therefore require monitoring and source data verification proportionate to their importance. Conversely, other data, for example participant demographic details not used in key analyses may present lower levels of criticality but should still be monitored and verified proportionately based on their potential downstream impact.

Ignoring criticality can create unnecessary burden without improving quality and may actually reduce quality by diverting attention and resources from what truly matters.

Sponsors and investigators are therefore expected to tailor their management and oversight to the criticality of the data, systems and processes specific to each trial.

Data, systems, and processes of higher criticality, where failures could meaningfully affect participant protection or the reliability of trial results, require a greater degree of management and oversight.

This increased intensity should take the form of increased focus, rigor, and timeliness in controls and decision making, while remaining clear, efficient, and targeted to the specific risks identified.

On the other hand, data, systems, and processes of lower criticality – meaning where failures would pose minimal risk to participant protection or trial results – could be managed with proportionately less management and oversight, avoiding unnecessary or complex controls that do not contribute to quality.

Let's briefly discuss key processes in a trial that would consistently require heightened attention and oversight proportionate to the criticality of the data throughout the entire data life cycle.

Attention should be given to:

- Processes to ensure the protection of the confidentiality of participants' data
- Processes to manage computerised systems to ensure they are fit for purpose and used appropriately – we'll cover this in Module 3.3.
- Processes to safeguard essential elements of the clinical trial, such as randomisation, dose adjustments, and blinding; and processes to support key decision making. This includes processes related to data finalisation prior to analysis, unblinding, allocation to analysis data sets, any changes in clinical trial design, and the activities of the Independent Data Monitoring Committee, or "IDMC," where applicable.

Oversight of these key processes should be carefully documented to ensure data integrity throughout the data lifecycle.

It is crucial to maintain the integrity of the blinding across all appropriate stages of the trial when it is part of the trial's design.

Protecting the blinding is not a one-time activity. It should be considered at every stage where data are created, accessed, reviewed, or analysed.

For example, maintaining the integrity of the blinding is especially important in the design of systems that capture, store, and transfer data. These systems should be designed and used in a way that prevents unintended access to unblinded information.

It is also a key consideration in the management of user accounts, specifically in determining who is permitted to view blinded versus unblinded trial data.

In addition, maintaining the integrity of the blinding is an important consideration in the delegation of responsibilities with respect to data handling and provision of data access at sites.

It is also an important consideration in data transfers, where care should be taken to preserve the blinding, for example, by ensuring that treatment assignment information is not included in datasets transferred to blinded parties.

Prior to any planned unblinding, database review activities should be conducted in a manner that maintains blinding.

Finally, statistical analysis must be performed with careful attention to blinding requirements.

That said, certain activities, such as interim analysis conducted by independent statisticians, may require unblinding, and in those cases, appropriate controls should be in place to ensure that unblinded information is only accessible to those who are authorised to see it.

At every step, the goal remains the same: to protect the integrity of the blinding and, ultimately, the reliability of trial results.

The potential for unblinding at every stage of the data lifecycle should be part of the risk assessment of a blinded trial.

We'll explore the data lifecycle more closely in Module 3.4.

One of the first steps in taking a risk-based approach to data governance is to identify the design elements, data, systems and processes that are critical to the quality of the trial.

Critical to quality factors are attributes of a clinical trial whose integrity, if compromised due to inadequate design and/or poor conduct, could jeopardise participant protection or the reliability of decision making based on the trial results.

It is important to recognise that critical to quality factors are identified for each individual trial and may evolve over the course of the trial.

What is considered critical in one trial may not carry the same level of importance in another, depending on the trial's design, endpoints, population, and operational complexity. As risks emerge or trial conditions change, critical to quality factors may need to be reassessed and refined to ensure they remain aligned with the trial's objectives, participant protection, and data integrity.

Consider the Crohn's Disease case example we introduced in Module 3.1. In this trial, all components of the co-primary efficacy endpoints are critical to quality factors because they drive the trial results.

Getting reliable endpoint data isn't just about what you measure. It's about how the systems and processes around that measurement are designed and managed to protect data quality and integrity.

Trials as complex as the one we see in this case necessitate a risk-proportionate approach to data governance across the data lifecycle, including system management, data collection, review, finalisation, and analysis.

This is where data flow diagrams can be useful. Let's look at the data flow for the 3 patient-reported CDAI components in order to identify data, systems, and processes related to data governance that are critical to quality.

This example is not intended to provide a comprehensive assessment of all critical to quality factors in this trial. It is intended solely to demonstrate the approach.

First, it is obvious that the ePRO data are critical to quality because they directly contribute to the co-primary endpoint of CDAI Clinical Remission at Week 12. If these data are not collected and managed reliably or if they contain errors, the integrity and reliability of the trial results may be compromised.

Now, let's identify two trial systems of higher criticality in this data flow.

The first one is the eCOA system, which includes the eDiary where participants enter their data, and the eCOA database where the data from eDiaries are transferred and maintained. This system warrants particular attention because it is a source of the co-primary efficacy endpoint data. Participants use the eDiaries to capture daily stool frequency, abdominal pain and well-being. The clinical investigator and delegated investigator site staff use the eCOA database to review the eCOA data and transcribe it into the eCRF, which calculates the CDAI score.

In addition, the service provider uses the eCOA system to manage this data.

The second critical system that we will highlight is the system that hosts, manages, and stores the eCRFs.

This system is used by investigator site staff to enter trial data, including all CDAI components. These include the 7-day pre-trial visit ePRO data, clinician-reported physical findings such as extraintestinal complications, anti-diarrhoeal drug use,

weight loss, and abdominal mass, as well as haematocrit values from the central laboratory.

In addition, the eCRF is programmed to calculate CDAI scores.

Both the eCOA and the eCRF systems are critical to quality because they are data acquisition tools used to collect and manage the co-primary endpoint data. Errors in design, validation, management, and use of these systems could have a significant impact on the quality of the co-primary efficacy endpoint data; thereby potentially impacting the reliability of trial results. We will discuss investigator and sponsor responsibilities for computerised systems in more detail in Module 3.3.

Now, let's identify a couple of critical processes.

In this case example, the data transcription process is a critical process because errors during transcription could compromise the accuracy and completeness of the CDAI data needed to calculate the CDAI scores. We will discuss investigator and sponsor responsibilities related to management of the data lifecycle in more detail in Module 3.4.

Another critical process in this case is ensuring that the eCOA system is used as intended. If the eCOA system is not used as intended in the trial, it could result in missed or incorrect data being entered, thereby compromising the reliability of trial results. Using the system as intended is critical to quality because it helps ensure accurate and complete data collection by participants and investigator site staff.

Once the critical to quality factors have been identified, the next step is to identify and evaluate potential risks to these factors. Appropriate risk control measures should then be defined and incorporated to mitigate or proactively prevent those risks. For data governance processes, this can include drafting of trial plans such as a data management plan, data review and data validation plans and a monitoring plan in addition to setting pre-specified acceptable ranges to support the control of risks.

We will return to this case and revisit these concepts and steps in Modules 3.3 and 3.4.

Thank you for completing Module 3.2.

Next, in Module 3.3, we'll look at the management of computerised systems and further examine risk evaluation and risk control as they relate to computerised system management.