

Magazine Article | March 1, 2019

---

## Using The QTA To Align Data -Integrity Expectations

Source: Life Science Leader

By Kip Wolf, Tunnell Consulting, @KipWolf



Outsourced GMP-regulated activities have clear requirements, including the use of quality-technical agreements (QTAs). While current FDA guidance “does not explicitly apply to the manufacture of investigational, developmental, or clinical trial materials, the FDA believes that quality agreements can be extremely valuable in delineating the activities of all parties involved in contract research and development arrangements.” The principles described in the guidance and here in this article may be applied to both commercial and precommercial stages of the product life cycle and to any relationship with suppliers that provide outsourced GMP-regulated activities. This includes CMOs/CDMOs as well as those that supply third-party laboratory and analytical services, as “cGMPs apply to all contract facilities, including analytical testing laboratories.”

According to EudraLex (i.e., rules and regulations governing medicinal products in the EU), any GMP-regulated activity that is outsourced “should be appropriately defined, agreed, and controlled in order to avoid misunderstandings that could result in a product or operation of unsatisfactory quality,” and “there must be a written Contract between the Contract Giver and the Contract Acceptor which clearly establishes the duties of each party.” When we expand the level of detail of the description around the duties of each party, particularly around specific transactions of data or information, we see much improved outcomes. Below are some examples of how data-integrity failures would present potential risks to product or operational quality for these commonly outsourced GMP-regulated activities:

1. mismanagement of clinical research data and metadata that will inform conclusions and content for the IND application, for the license application for new drug approval, and beyond
2. transcription of raw analytical data that is “substituted for the original source as raw data” and included in documentation (e.g., certificate of analysis) to support downstream processing.

Companies seldom take full advantage of the opportunity to use the QTA to further reduce risk through understanding and aligning on data definitions and standards of information exchange when on either side of a supplier relationship. Taking full advantage requires more than simply adding a section on data integrity, though. The QTA must be structured with data integrity in mind, as described in the examples below.

### **PREVENTABLE DATA-INTEGRITY FAILURES**

A QTA also represents an opportunity to clearly describe roles and responsibilities, inputs and outputs, and expectations from both sides of the contracted relationship. Clearly describing all elements of the roles and responsibilities of the contract giver and the contract acceptor for individual transactional activities will ensure process clarity and appropriately set expectations. The value of such goes beyond simply regulatory compliance and cost avoidance. It can provide tangible value in terms of error reduction, improved timelines, and increased revenue.

#### **EXAMPLE #1: DATES AND TIMING OF IND ANNUAL REPORTS**

A CDMO in a long-standing relationship with the multiple partners of a joint vaccine development program shared regulatory data between them (i.e., IND effective date) to facilitate planning for availability of clinical trial materials for study start and timing for submission of the IND annual report. To understand the data-integrity failure described here, we must first understand IND annual reporting requirements.

The IND annual report (IAR) is required to be submitted by the sponsor in yearly intervals “within 60 days of the anniversary date that the IND went into effect,” known as the IND effective date. This report is required annually until the final clinical study report for studies filed under the IND has been submitted to the FDA, or the IND has been withdrawn. Absent clinical hold, the effective date is calculated as 30 calendar days after official FDA date of receipt of the IND, communicated by the IND acknowledgement letter. This effective date is important both for earliest possible date of initiation of the proposed trial and for calculation of required annual reporting.

Only during parsing and transfer of regulatory data after the partners agreed to separate the joint venture did they realize that they had each been calculating the IAR due date differently. One partner calculated incorrectly based on 365 days after the date the IND was submitted, while the other partner calculated correctly based on 365 days after the IND effective date. This caused, at minimum, much confusion and required crisis management around IAR time frames that were not aligned between the two partners. As the reporting period defines the contents of the IAR (including cutoff date for contents), gaps, overlap, or confusion in the content reported may result, and this level of easily preventable error may cause additional regulatory scrutiny.

As the sponsor is responsible for defining the reporting period, some simple recommended additions to the QTA include:

- Define, explicitly, how due dates for regulatory report contents are communicated and how the content compilation process will be managed.
- Define the authoritative source of regulatory data (e.g., in what system owned by which partner would the IND effective date be considered authoritative, from which all others would reference it).
- Declare and agree to the appropriate IAR due date calculation and verify (through audit) that the calculations are accurate.

This example's recommendations also could apply in the commercial phase. The likelihood of this mistake occurring is increased by outsourcing and even more so in virtual companies, where interactions are very transactional. When GMP-regulated activities are outsourced, the "Contract Giver is ultimately responsible to ensure processes are in place to assure the control of outsourced activities" (see *Guide to Good Manufacturing Practice for Medicinal Products, Part I*). The QTA is the ideal location for defining input/output expectations for key transactions in the relationship. By defining critical data locations and metadata calculations in the QTA, this mistake could have been prevented.

## **EXAMPLE #2: DEFINING, UNDERSTANDING, AND INTERPRETING RAW DATA**

Multiple CMOs and contract labs were involved along the value chain through final disposition and release of the finished product. Assessment for conformance to file was performed in preparation for NDA submission, during which time both the batch-record-review process and the executed-batch records were examined in detail. Identical data elements (e.g., molecular weight on a Certificate of Analysis [CoA]) identified at different points along the value chain no longer matched.

It was found that the suppliers along the value chain each had different standards for the rounding of raw data and disparity in defining raw data. The contractor defined raw data incorrectly as the immediately preceding document from which data was transcribed.

For example, a contract testing laboratory would include a CoA in the batch record from the drug substance CMO to accompany release and transfer downstream to the drug product CMO. However, following the contractor's process, transcription of CoA data occurred to reflect the data in multiple places (e.g., email folders, batch record cover sheets, batch summary information, multiple cloud-based document libraries), where high incidents of error, a variety of rounding methods, and additional calculations were performed that changed the data's value when compared to the data on the CoA.

At the center of this data-integrity failure is the fact that the contract giver was provided copies of batch records by the contract acceptor, as opposed to being granted direct access to the batch records. The contract giver further confused the process by compiling data from various contract acceptors into a batch packet packet that included elements of the various batch records, CoA, and the like.

Some simple recommended additions to each QTA include:

- Declare the authoritative location for all batch records and define a process for review from that location.
- Agree on the standard definition of raw data and include it in the QTA.
- Define rounding and calculation standards for all specifications.

This data-integrity failure allowed errors and misinterpretations to occur that ultimately led to an extended batch record review that resulted in stock-outs and complicated the compiling, reviewing, and filing of the NDA submission, which was ultimately delayed.

## **DATA-INTEGRITY CONCEPTS THROUGHOUT THE QTA**

We recommend including in every QTA a standard section on data integrity, including updating existing agreements to the contemporary understanding of the regulatory landscape. Including a standard section that restates the common data-integrity principles (i.e., attributable, legible, contemporaneous, original, accurate), forces the conversation between the contracting parties and can help ensure all parties understand their responsibilities. It is worth the time and effort to prevent any types of data-integrity failures.

In addition to a section devoted to data integrity, evidence of the application of data-integrity principles should be pervasive throughout the QTA. In addition to the recommendations provided in the previous examples, other common suggestions are:

- Define clearly the authoritative sources of data and electronic documents, data-storage requirements, access and provisioning requirements, and any electronic signature requirements.

- Include process-flow diagrams, responsibility matrices, decision trees, and/or similar illustrations to aid in clearly defining and communicating any key transactional activities (e.g., batch-record review and disposition).
- Include data-integrity checks in any supplier-audit language or checklists.

*KIP WOLF is a principal at Tunnell Consulting, where he leads the data-integrity practice.*