Table 26: Data Integrity

Facilitator: David Good, *Eli Lilly and Company*

Scribe: Allison Lehtinen, *Pfizer, Inc.*

SCOPE:

2018 saw the issuance of two notable data integrity guidance documents. In March, the MHRA released "'GXP' Data Integrity Guidance and Definitions" and in December the US FDA released "Data Integrity and Compliance with Drug CGMP". Concurrent with the release of the guidance there has been increased scrutiny on data integrity during both inspections and submission reviews. Data integrity is a wide-ranging topic and even with a growing list of guidance documents, much implementation detail is left to the pharmaceutical industry. This roundtable aims to provoke a robust discussion on some of the more challenging aspects on the road to improving data integrity practices.

QUESTIONS FOR DISCUSSION:

1. What data is classified as "critical data', who makes that determination, where is it documented and how is determination defended?
2. What audit trails are reviewed? Who reviews them and on what frequency?
3. What are the best strategies for ensuring data integrity in submissions and for proving to regulators that complete data integrity exists?
4. What types of vulnerabilities in electronic systems and system architecture/administration have been identified and how can they be successfully mitigated?

DISCUSSION NOTES:

1. What data is classified as "critical data", who makes that determination, where is it documented, and how is determination defended?
    a. Identification of critical data, along with risk management processes are important to ensure data integrity
    b. Critical data could be limited to aspects that directly impact CQAs OR could be every single piece of data generated during a batch
        i. Anything you use to make a decision - Why acquire data if you are not going to make a decision with it?
    c. Requirements, SOPs, Quality Systems lay out requirements for data integrity
        i. May be necessary for commercial products or may be unnecessary burden in development
    d. Not every piece of data goes in BLA
        i. Some data are GMP, but some are not GMP - Should same data integrity requirements be placed on GMP and non-GMP data?
    e. Maybe originally was only GMP, but we are seeing this shift. There is no longer a line of demarcation between GMP and non-GMP.
    f. Example was provided that some biosimilar programs are looking at some non-GMP data (e.g., non-GMP sample handling and chain of custody).
    g. There have been significant inspection observations related to data integrity related to non-GMP data.

i. ALCOA principles still apply and all are important. How much risk are you willing to take on each of these based on where you are in the process development?
ii. Good science, good documentation practices, ability to trust the data are needed across the board.

h. What is being considered as GMP vs. non-GMP? Where do you draw the line?
i. Characterization data are likely non-GMP.
ii. Aspects that affect safety, purity, potency, etc. are GMP.

i. Level of documentation is not the same between GMP and non-GMP laboratories.

j. What about when you are using non-GMP data to make decisions about GMP material?
i. CQAs do not reflect all attributes of a product. Sometimes you only know things through characterization data.

k. GMP begins at development because you are using these data to inform decisions you are making about the future GMP product.
i. Hard to define which data are critical and which are not when you are early in development.
ii. Sometimes we depend on non-GMP data during investigations, etc.
iii. Early in development, you don't know what is critical, so you need to treat every piece of data as critical; therefore, data integrity just as important early in development.

l. The industry is typically risk averse - more data are better. But what do we do with all these data?
i. Some biotech companies are trying to push the envelope. Focus on scientific agility, good scientific practice.

m. Do all companies define "critical" in their SOPs/white papers, etc?
i. If not defined, this is a regulatory/inspectional risk.
ii. There is some interpretation of “critical”, so this needs to be defined for each individual company.
iii. How you use the data influences the assessment of "critical" data.

n. Are companies tracking trending with data integrity?
i. Software; data manipulation

o. EMPOWER was one of the first systems to be able to perform end-to-end

p. FDA considers all data included in the BLA as "critical" data. Criticality is subjective and depends on experience. Can even vary based on patient population. Needs to be considered from review side and from inspection side.
i. FDA knows that some analytical data are generated in development laboratory. But these data are important and meaningful in presenting the full story and in determining overall approvability of an application.

q. During GMP inspection, FDA is looking for traceability and consistency of data.
i. Results reported in BLA should be able to be traced all the way back to raw data.

r. Are there rounding issues, transcription issues, etc.? - FDA understands that these sorts of issues happen. Or are there true data integrity issues?

2. FDA inspection is looking to verify that company has control of the data - is the quality system robust enough to detect an error and then do something about it?

3. What audit trails are reviewed? Who review them and on what frequency?
a. NOT DISCUSSED

4. What are the best strategies for ensuring data integrity in submissions and for proving to regulators that complete data integrity exists?
    a. Some companies use cross functional teams to review all data in submissions.

5. What types of vulnerabilities in electronic systems and system architecture/administration have been identified and how can they be successfully mitigated?
    a. How to ensure data integrity of standalone systems?
    b. Sometimes difficult to find instruments that meet industry requirements for data integrity.
        i. Some software becoming outdated (e.g., move from Windows 7 to Windows 10)
        ii. Instruments/vendors claim to be compliant, but may not be in practice
    c. E.g., provide data in PDF format, but PDFs are editable
    d. Assessment of whether instrument is compliant depends on who you are talking with.
    e. Only person who can determine whether software system is compliant is a regulatory body (FDA, EMA, etc.).
        i. Vendors can only provide software that has capability to be compliant. It is then up to the users to enforce/control the compliance aspect.
    f. Issue: Sometimes sponsor representative is communicating instrument/software issues and vulnerabilities to the vendor, and the vendor has never encountered this issue before.
        i. There needs to be a collaborative relationship between sponsor and vendor.
        ii. Would be nice to see routine software updates from the vendor that mitigate these identified issues.
    g. User privileges and access control issues: May need to have organizational shifts so that software admins and users are not the same person. This is important to ensure data integrity.
        i. The users should not be able to have administrator privileges, as this is a data integrity issue if the user can manipulate the data.
        ii. This creates an issue because the software experts are typically the users. If someone less experienced is the administrator of the software, they likely do not have the knowledge to troubleshoot the issues.
    h. How are companies providing training on the systems?
        i. Scientists/users are not trained in IT.
        ii. IT department is typically not trained in the regulations and requirements.
        iii. Some vendors provide privacy security manuals with their instruments - can be shared with IT department. This is beneficial for small companies who can work quickly to get instruments up and running.
        iv. Some companies have a business-IT partnership model which define the parameters/requirements for the business users. IT department can then assess the gaps with the systems and software to update and make decisions on what systems need to be brought on or retired.
        v. Data integrity training within the systems (hands on training) is important - how to look at the audit trails, history, etc.
    i. This is important training for reviewers/data verifiers.
    j. Should provide similar training with the instruments themselves.
    k. Raw data - traceability and accessibility
        i. This is difficult sometimes, especially during early development with standalone systems.
    l. Often need specific software to access and read the data that were generated. How to ensure data integrity if the software is obsoleted, the vendor goes out of business, etc? How to maintain traceability and reproducibility of the raw data?

i. Are companies implementing second person verification to overcome these instances of obsolescence?

m. Some companies are implementing second person verification in micro testing - both for batch release and environmental monitoring.

n. Digital direct connections in chemistry laboratories often obviates the need for second person verification. However, for tests that may not have these direct connections, second person verification should be implemented.

o. Difficult/challenging to perform this level of more verification with fewer people.

6. May consider moving to a model of selecting a percentage of samples to be confirmed with second person verification.

a. Open questions (future roundtable topics):

i. How to ensure data integrity with 3rd party vendors/contract laboratories/outsourced testing?