About ISPE   Knowledge & Learning   Pharmaceutical Engineering Magazine

Communities of Practice

ispeak

Home   Knowledge   Regulatory   Annual Meeting   FOYA Program   Contribute

Home » ISPE Annual Meeting » Knowledge » You are reading »

Data Integrity, Critical Thinking & MHRA 2017, Oh My!

👤 ISPE   🕐 October 12, 2016   📄 ISPE Annual Meeting, Knowledge   💬 No Comment

On Monday 19 September, the Information Systems track at the 2016 ISPE Annual Meeting & Expo explored critical thinking skills, analytics in data integrity, and MHRA 2017 data integrity requirements.

A Key to Success

The session began with a presentation by Monica Cahilly, President, Green Mountain Quality Assurance LLC.

"Most of you are scientists," she began, addressing the audience. "In school you preferred multiple choice to essay questions, right? Well, this is presentation is about the essay portion of the test: critical thinking skills.

Search

[Search …]   [Search]

Subscribe

Subscribe to ISPEAK and receive notifications of new posts by email.

[Email Address]

[Subscribe]

Feature

"The workforce of the future will require people with critical thinking skills," Cahilly continued. She referenced Wall Street Journal articles that declared "Employers Find 'Soft Skills' Like Critical Thinking in Short Supply" and "Bosses Seek 'Critical Thinking,' but What Is It?"

"Everybody wants critical thinking," she said, "but we may not have been taught this in school."

Critical Thinking

Critical thinking is a self-examining, self-aware, intellectually disciplined process of evaluating information from a variety of perspectives to yield a balanced and well-reasoned answer.

Critical thinking helps us see data, Monica said. "Unless we develop these skills, our ability to see is limited by our biases, assumptions, history, culture, emotions, and many other factors. We could go through our lives recycling ourselves to ourselves, but never really seeing what's going on in reality."

At the FDA Basic Drug School, investigators are trained in critical thinking because it allows them to see risk more quickly. The European Medicines Agency Questions and Answers on Data Integrity published in August 2016 says that "[t]he application of critical thinking skills is important to not only identify gaps in data governance, but to also challenge the effectiveness of the procedural and systematic controls in place."

Critical thinking is an important component of data integrity.

Increasing Focus

Data integrity is under increasing focus because of evolving business models, increasing globalization, complex and interdependent supply chains, increasing use of technology, and increasing use and availability of data. "It's a hot topic in all industries," Monica said, citing examples from the automotive industry. "All were a result of unreliable data."
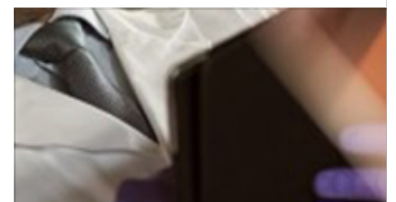
In the pharmaceutical industry, the relevance of data integrity is its impact on patient safety and product quality. "Those are our first missions," Monica said.

"So how did we get to product shortages and substandard manufacturing environments?" she asked. "Did people see the problems but not have the courage to speak up? Or did they not see the risks?"

Seeing Risk

Critical thinking should be part of a holistic risk-based approach.

"Healthy companies realize that risk is going to happen," Monica explained. "When you look deeper you find it, and can manage it. But unhealthy companies avoid this. A pattern of data that's 'too good to be true' probably means that the company has blind spots or isn't' looking for risk.

"There will always be 'residual risk,' and it's important to recognize this," Monica noted. "It means embracing imperfection. Zero tolerance actually increases risk unless you have infinite resources—and no one has that. So we're always taking on imperfection."

Blind Spots

A risk-based approach to data requires critical thinking skills—but what are the reviewer's blind spots? "Too often people throw out data that doesn't match what they expect to see," Monica explained.

She cited an example using the famous 1915 William Hill Ely illustration "My Wife and My Mother-In-Law."

When looking at this picture, most Western viewers see either a young woman or an old lady. When American counterterrorism forces used this illustration as part of their international training, foreign military partners saw a bird.

"When you try to make meaning from data," she said, "you'll code it with something that's already in your database. Having terms for objects means you'll identify them faster."

Critical Thinking in Data Review

So what do we focus on? "Identify those processes and data that are critical to assure human subject protection and the reliability of study results," said Monica. "Ask yourself: What is the aberrant data? What could harm patients? How many replicates do I need for an outlier?"

Source: Library of Congress Prints and Photographs Division, Washington, DC.

To answer that last question, Monica used another example. "If you want someone to see data with critical thinking skills, pair it with an emotional anchor. Let's say I have four pieces of candy. The first one's poisonous, but pieces two and three are OK. Would you eat the fourth? No. You know that's not a statistical outlier with sufficient certainty.

"Or imagine that I sliced into a beautiful birthday cake and found a piece of glass," she continued. "Would you eat another piece of that cake?"

Monica said that we can develop and expand our ability to see data with training, and by adopting Descartes's idea of "sound evidence."

We can also open ourselves to alternate viewpoints. While the way that we see (or don't see) has a lot to do with our underpinnings, we can connect with people in a way that expands our perspective. It's important, however, that you don't simply skew to that viewpoint instead, she cautioned.

"A critical thinker realizes there's a relationship between knowledge and the knower, and this is always changing," she added.

Using Analytics to Detect Data Integrity Issues

Mark E. Newton, Associate Senior Consultant–QA, Eli Lilly and Company, Indianapolis, and a leader of ISPE's Data Integrity Special Interest Group, explored the use of analytics to detect data issues.

Integrity issues can arise from a number of factors, including manual data entry, shared system access, and lack of an audit trail. "Ask yourself: 'What's wrong with the method if we have to integrate manually? And an audit trail can tell you if the integration was calculated multiple times— or if someone was trying to manipulate the data," Newton said.

Regulators expect oversight, and expect firms to routinely look for improper activities as part of review. "We often lack the tools to get the job done, however," he continued. "It's like looking for a needle in a haystack. So we reduce the size of the haystack to a more manageable level."

Analytics can assist in quality oversight and highlight conditions that merit review. While this is helpful, using them indiscriminately can bury companies in data—and allow real signals to be missed. "It's best to start small," Mark said, "and assess the value of each analytic after a trial period."

"What reports can I generate that I can use to find data integrity issues?" he asked the audience.

Sample analytics:

- **Right first time:** Indicates a sample that requires reprocessing; can illuminate trends in methods, materials, or analysts with rework rates above the rest of the population.
- **Multiple test runs:** Lists samples with results from multiple test runs. This can help indicate those that merit attention, or identify

analysts that keep performing runs until they get the desired
result.

- **Manual peak integrations:** Counts manually and auto-integrated peaks, and shows how to improve efficiency by reducing manual processes.

- **Reprocessed run:** Doesn't necessarily indicate a data integrity problem. Who's the analyst? Maybe it's an education issue.

- **Manual integration detail:** Lists peaks with manual integration and counts audit trail entries; this can identify injections with more manual intervention, which may warrant closer review.

- **Short run:** Lists sample runs with a small (one or two) number of injections. Users "testing into compliance" will inject sample solution multiple times, often in short runs.

- **Access changes:** Lists access changes for all system users; it could indicate improper role changes and conflicts of interest.

- **Access roster:** Shows how many users are represented in each role. Roles with enhanced access deserve close scrutiny. Administrators should be checked for conflict of interest.

- **Aborted run:** Why was the run stopped? There are a lot of reasons this can happen, but it's important to find out why, because this is an unusual event.

- **Demo/test/trial:** Finds samples with suspicious names (like demo%, test%, or trial%). Even if it's a proper activity, find out why users are doing this in a GxP environment—it's a bad practice.

The bottom line, Mark said, is that while analytics can help identify issues, each suspect record requires human confirmation. It's also important to review enforcement findings for ideas. Ask yourself: "How would we detect that?"

Preparing for the MHRA 2017 Data Integrity Requirements

The last session was a discussion by George Bass, Head of eCompliance and Data Integrity at Alcon, a Novartis Company, about controls

mandated by the March 2015 MHRA data integrity guidance. The 2016 revision, published 18 months later, addressed gaps in the 2015 guidance, changed 11 existing definitions, added 6 new ones, and clarified expectations.

Two specific technical controls must be in place by the end of 2017:

- **Audit trails:** Review must be part of the routine, and must incorporate good documentation practices for corrections and asset control.

- **Access controls:** System access must be unique for each user, and must be as a user or an administrator—one or the other. A paper alternative is permitted if traceability demonstrated. Bass described a process of data governance, process assessments, and data review that would enable putting these MHRA-required technical controls in place by the end of 2017.

- **Data governance:** Leverage existing quality management system procedures where possible, address intentional and unintentional breaches, define data ownership, with zero tolerance of data integrity issues.

- **Process assessments:** Design the process with data integrity in mind. Put clocks on the floor so people can note date and time. Eliminate loose pieces of paper and sticky notes. Design processes so that it's easy to get to and record the data.

- **Data review:** Documents review, defines correction process, and demonstrates compliance with ALCOA principles.

Without the right infrastructure—including senior management support, training, and the development of a culture in which data integrity is embraced—a system to put the technical controls in place is not possible.

Data integrity will continue to be a hot topic, George said, until the industry has sufficiently matured its approach to all data relevant to products and their approval, and regulators are confident that they can trust the data they review.

RELATED POSTS

[Creating Supply Chain Excellence Part 2](#)

[Making an Impact in Pharma Industry – 2016 ...](#)

[Data Entry in a Pharmaceutical Data Integrity Envi...](#)

[Reading Roundup: Top Blog Posts from September 201...](#)

🏷 2016 ISPE Annual Meeting & Expo, data integrity

No Comments Yet

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

	Website

Post Comment

☐ **Notify me of follow-up comments by email.**

☐ **Notify me of new posts by email.**

« Creating Supply Chain Excellence Part 2

Copyright ©2016. ISPEAK

About ISPE   Knowledge & Learning

Pharmaceutical Engineering Magazine

Communities of Practice