PHARMACEUTICAL ONLINE

BEST PRACTICES TO ENSURE DATA INTEGRITY IN YOUR PHARMA SUPPLY CHAIN

PHARMACEUTICAL
ONLINE

As the pharmaceutical world is becoming more data-driven, you'll need to pay closer attention to how your pharmaceutical company's culture and operations ensure the completeness, consistency, and accuracy of data. Data specialists call this data integrity. Such data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA), according to the FDA. Similarly, data must be complete, consistent, and accurate throughout the data life cycle, according to the Medicines and Healthcare products Regulatory Agency (MHRA) and the Pharmaceutical Inspection Co-operation Scheme.

The first section of this e-book provides recommendations on people-related advice. The first article gives more of an introduction on what data integrity is and examines how your company's quality culture can assure data integrity. The following article shares five misconceptions about what data integrity is and is not. The next article shares eight steps for your company to prepare for the FDA's upcoming "data effect" tsunami, and those steps include both people-related and technology-related steps.

The next section of the e-book delves into best practices for data integrity along the pharmaceutical value chain, including what to audit in laboratory information management systems (LIMS) and how to prepare for that audit, important cGMP considerations for implementing electronic batch records, how to audit electronic batch records, and how to address data integrity in your supply chain risk management. The e-book concludes in sharing nine pitfalls to avoid as you journey deeper into today's world of data integrity.

PHARMACEUTICAL
ONLINE

CONTENTS

HOW TO ENSURE YOUR QUALITY CULTURE ASSURES DATA INTEGRITY

Chris Smalley

Pharmaceutical and Compounding Pharmacy Consultant

Data integrity (DI) is receiving greater attention, and deservedly so. Data, given appropriate context, become knowledge, and knowledge of the processes and products is invaluable. To be able to rely on that knowledge, data must have integrity. One solution is to automate the process, essentially removing the human element. But not all instances of data generation/capture can or should be automated. With humans – our team members – engaged in data generation/capture, the quality culture is a major pathway to assuring our data have integrity.

First, let's review: What is data integrity?

- ***Data integrity*** refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate ***data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate*** (ALCOA), according to the FDA.
- Data must be complete, consistent, and accurate throughout the data life cycle, according to the Medicines and Healthcare products Regulatory Agency (MHRA) and the Pharmaceutical Inspection Co-operation Scheme.

The industry has accepted an expanded definition of DI, ALCOA+, which adds *complete*, *consistent*, *enduring*, *and available*. For this article, the focus will be on the original ALCOA expectations because that is squarely where data generation/capture is addressed.

Many employees are not involved in the capture or generation of data, but rather are involved in the review, analysis, storage/archival, disposition, and other steps in the life cycle. Although the focus here will be on capture/generation, these other areas will also relate to the role of quality culture.

As a beginning, it is important to review the definitions of those terms that constitute ALCOA:

- **Attributable:** It should be possible to identify the individual or computerized system that performed the recorded task. The need to document who performed the task/function is, in part, to demonstrate that the function was performed by trained and qualified personnel. This applies to changes made to records as well: corrections, deletions, changes, etc.

- **Legible:** All records must be legible – the information must be readable in order for it to be of any use. This applies to all information that would be required to be considered complete, including all original records or entries. Where the "dynamic" nature of electronic data (the ability to search, query, trend, etc.) is important to the content and meaning of the record, the ability to interact with the data using a suitable application is important to the "availability" of the record.
- **Contemporaneous:** The evidence of actions, events, or decisions should be recorded as they take place. This documentation should serve as an accurate attestation of what was done, or what was decided and why, i.e., what influenced the decision at that time.
- **Original:** The original record can be described as the first capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state.
- **Accurate:** Ensuring results and records are accurate is achieved through many elements of a robust pharmaceutical quality system. This can be composed of:
    - Equipment-related factors such as qualification, calibration, maintenance, and computer validation
    - Policies and procedures to control actions and behaviors, including data review procedures to verify adherence to procedural requirements
    - Deviation management, including root cause analysis, impact assessments, and CAPA
    - Trained and qualified personnel who understand the importance of following established procedures and documenting their actions and decisions.

Together, these elements aim to ensure the accuracy of information, including scientific data that is used to make critical decisions about the quality of products. Keeping these elements in mind, let's now move to the role of quality culture.

WHAT IS THE QUALITY CULTURE IN YOUR ORGANIZATION?

If you took a poll in your organization, will employees be honest or provide the answer they think you are looking for? After all, aren't we all *team players*? Organizations have embraced faddish phrases that superficially seem good but have little to no impact on the quality culture.

So, how do your employees perceive the culture? In fact, what if you could get in the heads of your employees? Would they be thinking:

1. If I get caught making a mistake, I'll be disciplined or fired;
2. It's not my job;
3. I'm only a cog in the big machine; ***or***
4. I'm a valued employee who has the resources I need to succeed at my job?

If you think their perception is anything other than #4, then read on!

TRAINING IS ONE ASPECT OF CHANGING AND MAINTAINING THE QUALITY CULTURE

Training in quality culture is not having employees read SOPs online, nor is it having them sit in a classroom or, worse, an auditorium to be lectured at. What training in a quality culture means is:

- Conducting interactive workshops;
- Using facilitators who are not their supervisors or managers; and
- Seeing that their management is committed to the training.

A key element in the training is to explain not just the what but the why. Reading SOPs and hearing lectures does not engage the team members in a way that helps them understand the why. Interactive workshops, made even more valuable when conducted as a multidepartment activity, will assist in providing the team members with a broader perspective of the process and an understanding of their role. Training that is led by supervisors or managers many times will not result in questions from team members, who may think they will be judged for asking an "obvious" question. With a facilitator (from another department, from a trained member of your HR team, or a third party), however, the group can relax and ask those questions that can lead to deeper understanding. Seeing that management is committed to training, not just by paying lip service but by demonstrating commitment by attending the training, devoting the time and resources to provide quality training, and using feedback from training, will improve processes and procedures. For team members who understand the importance of their job, not only the process but the final product and the impact on the patient who receives it, we see a *tremendous* difference in their attitude toward data integrity. Why? Because they understand the importance of their role, their contribution.

The key here is communicating to everyone involved an understanding of their role in the product that is passed to the next step (our "customer"), as well as their role in the product that the clinician or patient receives (our final goal).

ENSURING EMPLOYEES HAVE NEEDED RESOURCES

Ensuring appropriate resources means:

- ***Equipment is available, qualified, and calibrated:*** Having equipment available when the team member needs it means their time is valued. Having equipment that is qualified and calibrated means they have the tools they need to do a good job, and the data generated will be correct.
- ***There is adequate time to perform the task:*** Adequate and appropriate resources contribute to a good quality culture. For example: Adequate time to perform the task means they are not rushed, and they have the time to perform the task correctly.
- ***They have a "buddy" checking on them:*** This doesn't mean a supervisor checking up on them. It means someone stops by periodically if they are working alone, to see if they are safe and to ask, "Do you need a hand with anything?"

A Hypothetical Case Study: A laboratory chemist receives samples from two batches toward the end of the day on Friday. This chemist made a promise to their child that they would take them to their soccer game. By the time the tests are completed on the first of the two batches, it is very close to the time the chemist would need to leave at the end of their regular workday. The organization has made clear that it doesn't like samples stored and tested later. The chemist rationalizes that both batches were made by the *same* team on the *same* equipment on the *same* day, so they rerun the test results report after resetting the batch number and time and, consequently, can leave on time to get to the game.

Who is in control of the quality culture? In this example, it is the people responsible for scheduling and workload. If samples are scheduled to come into the lab late in the day, perhaps there should be a second shift. Maybe if the scheduler/planner added another batch to the Friday schedule, then overtime should have been planned and people could make the choices in their work/life balance. But understand that putting a person into the predicament described above can result in poor choices, leading to issues with data integrity and questionable quality.

Do your team members have the resources? Do your team members have the time to do their jobs properly? Do your team members have quiet space to concentrate when needed in performing tasks like document review? Do team members, when working on a prolonged task have someone perform a buddy check to see that they're doing OK and they're not some forgotten cog in the machinery? These examples illustrate the intersection of *quality culture* and *data integrity* that prevents team members from having to make bad choices.

In conclusion, as management, data integrity is important – it provides knowledge of the process and is a compliance item. A quality culture will ensure DI, and you can build a quality culture by helping team members feel valued, understand their role/contribution to the product and that the ultimate customer of the product is the patient, and by providing the resources they need to perform well.

ABOUT THE AUTHOR

Chris Smalley, Ph.D., is a consultant for ValSource, Inc. focused primarily on compounding pharmacies. His expertise includes single-use systems and aseptic operations. Previously, he was director of quality operations for Wyeth Pharmaceuticals for 12 years, responsible for setting validation standards and validation activities globally. His research experience includes responsibility for quality in the U.S. operations of the Sanofi Research Division, and earlier he worked for Johnson & Johnson as a plant manager. Smalley has been a member of the PDA Board of Directors and the PDA Science Advisory Board. Currently, he is a member of the ISPE Disposables Community of Practice.

5 MISCONCEPTIONS ABOUT DATA INTEGRITY IN PHARMACEUTICAL AND DEVICE DEVELOPMENT & OPERATIONS

Peter H. Calcott, Ph.D.

President & CEO, Calcott Consulting LLC

Data integrity (DI) as a topic or focus is not new: It is the foundation of basic research as well as the development of medicines. Patients and customers expect us to approach the science of drug development honestly and trust us to do it correctly. It is the cornerstone of our business, which is based on trust. However, in 2015, the Medicines and Healthcare products Regulatory Agency (HMRA) issued a landmark guidance on the topic of DI and problems it had seen in the industry during inspections.[1] This was reinforced by further guidances issued subsequently by the Food and Drug Administration and the European Medicines Agency and again by MHRA, both in 2016 and 2018.[2,3,4,5] But DI issues are not new. I have personally experienced them over my career, starting almost 40 years ago. They have always been there, but it appears they may have increased in frequency more recently, thus moving the issues to the forefront.

This two-part article series is not going to be a rehash of these very valuable guidances, which have been issued and implemented in most companies over the last few years. Rather, this article series is going to focus on my experience as a consultant who goes into companies to audit or perform gap assessments of systems and will illustrate some of the pitfalls companies fall into in the development of a rugged DI strategy. That includes misconceptions (this article, part 1) as well as poor implementation practices (my next article, part 2).

MISCONCEPTION 1: DI ISSUES CAN ALWAYS BE TRACED BACK TO NUMBERS.

One of the first misconceptions is that DI issues always involve problems with numbers, so they are limited to the QC labs and the production shop floor. While there are numerous cases of DI transgressions involving numbers, there are many where numbers do not feature at all in the real issue at hand. A case in point is in the writing of validation reports and investigations. Often in validations and investigations, we get information that does not fit the preconceived expectations. This must always be evaluated, discussed, and featured prominently in the discussions and conclusions. I have found a tendency to "hide" these issues, hoping people just do not notice. The DI issue can start as a number issue, but often it escalates to wrong conclusions and wrong decisions that are not supported

by the numbers that are there. These anomalies or deviations must be analyzed and persuasively discussed so we can truly assure they do not impact the conclusions and validity of the reports.

MISCONCEPTION 2: DI ISSUES ARE INTENTIONAL.

When you examine warning letters, you are left with the feeling that in these cases it is most probably intentional events that have been uncovered. However, in my experience, the majority of cases I have encountered have been unintentional errors – honest mistakes. A case in point happened when I examined a validation report of a computer system the company claimed was Part 11 compliant 6. In this case, a stress test of the system was ill conceived and executed such that the conclusion was not supported by the testing. When pointed out, the IT professional was shocked and immediately set the ball in motion for remediation of the system as well as others where they suspected the same issue might apply. So, when you start an investigation on a suspected DI issue, do not assume the worst of the persons involved. Give them the benefit of the doubt until you are really certain it is intentional.

MISCONCEPTION 3: DI ISSUES ARE CONFINED TO E-SYSTEMS.

We all know that DI issues can occur in paper-based systems as well as e-systems and we know that the issues will manifest in different ways. We also know that the remediation can be quite different in the two situations. However, I have seen in many cases when the FDA has cited a company for DI issues; the remediation has focused overwhelmingly on assessments of e-systems. The company will create inventories of e-systems and methodically check them against Part 11 compliance criteria.[6] However, not all DI issues are labeled DI issues in FDA citations. In some cases, the FDA may just reference poorly executed investigations that do not support the conclusions or they may reference quality issues by not reviewing documents adequately enough. There is no mention of DI issues; they are just not doing their job adequately. Yet these are paper-based examples of DI issues. What is often missing in many responses is the real recognition that DI issues can occur in paper-based systems that have nothing to do with Part 11 compliance. In these cases, there is no risk assessment of these paper-based systems or processes to identify weak points worthy of remediation.

MISCONCEPTION 4: IT'S A COMPUTER PROBLEM.

The agencies have been very forthright in identifying DI issues as a people problem.[1-5,7] What they mean is that it is people who cause the DI issues. With paper-based systems, it is very much clearer because people are actively engaged in the activities. The causes of these "human errors" are broad and can be due to many factors, including workload, effectiveness of training, and culture in the company, just to name a few. In the case of e-systems, many people indicate that it is the e-system that has failed. But that misses the point. It is people who evaluate systems, choose systems, configure them, validate them, test them, and ascribe access to the users. A failure in any one of these elements can render the system to being vulnerable to DI issues. I have seen many cases where the system administrator has assigned the wrong access level to an employee, giving them more access than the job requires or needs. Stress testing of systems is often found lacking in validations. I have also seen acceptance of vendor IQ/OQ that is substandard. As the saying goes, "buyer beware." In most cases of DI problems, it can be traced to a human error or incomplete assessment.

MISCONCEPTION 5: MANAGEMENT AND COMPANY CULTURE DON'T PLAY A ROLE.

In the guidances quoted on DI and its issues, the regulatory agencies are adamant: Management sets the tone and culture of the company and determines whether DI will be problematic or not. It is paramount that the prevailing culture in the company is one that focuses on the patient in assuring the delivery of a safe, efficacious product on time. With this focus on the patient, a blame-free culture that is open, where operators can raise issues without fear, must prevail. Operators in production or the QC labs must recognize that the right result of an operation or test may not result in the product being released. The right result may end up rejecting the material. The right culture is one major step in assuring an effective DI strategy that works.

REFERENCES

1. MHRA GMP Data Integrity Definitions and Guidance to Industry March 2015
2. FDA Data Integrity and Compliance with GMP April 2016
3. EMA Data Integrity August 2016
4. MHRA "GX" Data Integrity Guidance and Definitions March 2018
5. FDA Data Integrity and Compliance with Drug CGMP December 2018
6. 21 CFR Part 11 Electronic Records; Electronic Signatures — Scope and Application
7. PIC/S Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments July 2021

ABOUT THE AUTHOR

Peter H. Calcott, D.Phil., is president and CEO of Calcott Consulting LLC, which delivers solutions to pharmaceutical and biotechnology companies in the areas of corporate strategy, supply chain, quality, clinical development, regulatory affairs, corporate compliance, and enterprise e-solutions. He has also served as an expert witness. He also teaches at the University of California, Berkeley in the biotechnology and pharmaceutics postgraduate programs. Previously, he was executive VP at PDL BioPharma, chief quality officer at Chiron and Immunex Corporations, and director of quality assurance for SmithKline Beecham and for Bayer. He has also held positions in R&D, regulatory affairs, process development, and manufacturing at other major pharmaceutical companies. He has successfully licensed products in the biologics, drugs, and device sectors on all six continents. Calcott holds a doctorate in microbial physiology and biochemistry from the University of Sussex in England. He has been a consultant for more than 20 years to government, industry, and academia.

ARE YOU READY FOR THE FDA'S "DATA EFFECT" TSUNAMI? 8 STEPS TO PREPARE

Matt Collins

CEO, Cignyl.

John Giantsidis

President, CyberActa, Inc.

The FDA is moving forward with its Data Modernization Action Plan (DMAP), the next leg of the Technology Modernization Action Plan (TMAP). Announced on March 3, 2021, DMAP is the agency's overhaul of technology and data with the objective of bringing together increasingly disparate and diverse data sources to help understand and pinpoint emerging public health threats.

This sounds very noble, and using data as the basis of the FDA's regulatory decision-making seems to be an improvement. So, why would this be a tsunami for biotechnology, pharmaceutical, and medical device manufacturers? Do not misunderstand, data turned into knowledge improves understanding, decision-making, and, ultimately, outcomes. Businesses have learned this and are continuously improving their use of analytics as a competitive differentiator. However, what makes data valuable and informative can also be dangerous when wielded by a novice or used without proper verification and governance. On paper, the DMAP outlines several aspirational efforts to bring together a massive number of disparate data sources. What DMAP fails to address are the associated risks that come with predictive algorithms and poor modeling.

Predictive analytics and modeling are a form of artificial intelligence (AI). Predictive analytics uses machine learning to predict outcomes using historical data. Machine learning is an AI technology that finds patterns at scale with data sets. With machine learning, the models used to create predictions can act as black boxes. This means that how the predictions came to be is not fully understood. And while there are many instances of positive experiences with black-box algorithms, there are cautionary tales of algorithms gone bad. Let's be honest, the FDA does not always take an innocent until proven guilty approach with manufacturing firms.

The time is now for manufacturers to prepare themselves for the influx of questions, audits, observations, warning letters, and more with this new proclaimed approached to maintain data-driven regulatory decision-making.

Before we outline a road map to prepare for the incoming storm, we must discuss how social media will influence the FDA's modernization of information. OpenFDA is an excellent source of FDA data accessible to the public (note the warning to avoid using this information in making medical decisions).

The goal of providing data access to all puts manufacturers in the driver's seat to better control their destiny. What is missing? There are over a quintillion bytes of data generated daily with social media outlets.1 Most social media information (e.g., Twitter, TikTok, Instagram, reviews on Amazon, etc.) does not apply to manufacturers. However, there is a small percentage of this information that significantly impacts your business. Guess what? The FDA plans to monitor and assess this information under the umbrella of protecting public health. To prepare for this broad sweep of informational overload, manufacturers need to expand their post-market system capabilities by creating their own manufacturer Data Modernization Action Plan (mDMAP). Here's the eight-step method to create your own mDMAP.

1. WALK THE WALK WITH PREDICTIVE ANALYTICS

Many manufacturers proclaim they have predictive capabilities, but instead they outline archaic approaches toward demonstrating state-of-the-art devices, made under state-of-the-art conditions, with state-of-the-art outcomes. Repetitive descriptive statistics only tell the history and remain a passive approach to post-market monitoring of signals. Descriptive analytics does not facilitate the much-needed dynamic monitoring. Without dynamic monitoring, manufacturers cannot proactively respond to information and prevent significant business disruption. The FDA is going predictive. Manufacturers need to prepare themselves to stay ahead of the curve. Instituting mDMAP can be a source of competitive advantage and significantly decrease the time spent writing fiction as to why your devices remain the best of the best.

2. INSTITUTE NEW CAPABILITIES INTO YOUR POST-MARKET SURVEILLANCE LISTENING SYSTEMS

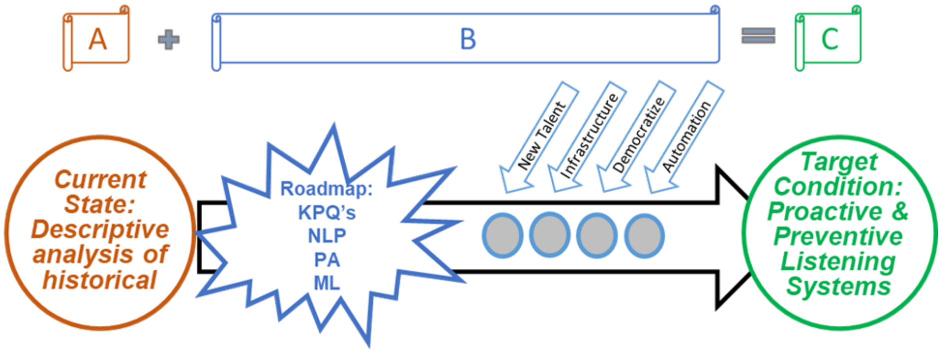
This will bolster your ability to respond to user experiences with your competitive devices (your opportunity to make quality a competitive advantage). As your mDMAP program evolves, your business vernacular will need to standardize around machine learning, predictive algorithms, and predictive intelligence. mDMAP is your way to get intimate with new data sources and new ways of seeing the information. Avoiding this intimacy increases your risk of "for cause" audits (we all know these audits go well!).

The bulk of new data is unstructured, which means the data is not conveniently in the form of a table with structured rows and columns. It is textual, video, pictures, etc. This lack of structure makes it difficult for the quality professional to understand, evaluate, and use it to support prevention. However, anything worth having is typically difficult at first. Unstructured data represents your new gold mine for post-market enlightenment. Anyone connected to the internet can voice their opinions. The ability to listen means manufacturers need to optimize their listening systems.

3. USE THE A+B=C FORMULA

Given that we understand A (your current post-market listening system state) and C (the future post-market listening system state), we can solve for B (what you need to do to stay ahead). The same thing goes for our ability to transform our post-market listening systems and predictive analytics program. The first step of a great mDMAP approach is to outline your targeted future state (or variable C). To create a targeted future state, paint a picture of the destination (what you want to accomplish). Next, define your current state (or where you are currently sitting, variable A). Painting a realistic picture of the current state is difficult for many manufacturers, as it requires a lot of arduous self-reflection and realizations. What are your current capabilities, what are your current data sources, do you have a quality warehouse or data lake? By outlining the current post-market state and painting a picture of the destination, you effectively can solve for B – how to achieve your new mDMAP realities.

Figure 1. Road map to mDMAP


A
+
B
=
C
New Talent
Infrastructure
Democratize
Automation
Current State: Descriptive analysis of historical
Roadmap: KPQ's NLP PA ML
Target Condition: Proactive & Preventive Listening Systems

Variable B represents the road map from your current condition to the mighty target condition. Transforming your post-market listening systems and predictive capabilities requires investment in your infrastructure and some sweat equity. Before you begin building, the path to enlightened post-market and predictive systems begins with a cross-functional assessment of key performance questions (KPQs). Many people and businesses jump right to KPIs (key performance indicators), but the rocket fuel in any analytics program begins with KPQs.

4. DEVELOP YOUR KEY PERFORMANCE QUESTIONS

Your ideal KPQs will allow you to develop a customized suite of information that delivers exactly what you need and avoid the traditional report on everything where you learn nothing. KPQs need to be open-ended (as they are questions) so that the team can determine:

- Which KPI answers the question?
- What type of data is necessary to create the KPI?
- Where does this data reside?
- Do we have access to such data?

Capturing the answers to these questions through a simple matrix helps to archive the knowledge, aligns the organization, and, most importantly, allows a new person to understand the intelligence behind the data analysis. You will be amazed at how powerful such a simple document becomes with immediate improvement to an existing post-market intelligence system. Having a prepared, yet simple and solid starting point, succinctly aligns the organization on your impending journey toward mDMAP bliss. Additionally, put this matrix in an existing procedure and be amazed at your ability to tame outside regulatory authorities.

5. BRING IN NEW SKILLS AND CAPABILITIES (PEOPLE TALENT)

As people leave the organization or the business grows, the organization must focus on different skills and capabilities. As people exit the organization, we typically replace them with others with a similar skillset. Our mDMAP journey requires a more thoughtful approach to new employees. Use these opportunities to look for the skills needed to drive your future state. An excellent method to support skill requirements is to draw three circles and outline three high-level skills required. As an example:

- Circle 1 = Domain expertise (e.g., quality, regulatory, technical, etc.)
- Circle 2 = Computer hacking (e.g., programing skills such as Python, R, or data analysis skills with Power BI or Tableau)
- Circle 3 = Math and statistics (e.g., multivariate, uni and bivariate, etc.)

Once you have your three main topics, you can add subcategories within the circles. Why use three circles? It is easier to digest how to think about the future skills needed using such an approach. Jumping into a job description makes it easy to fall into the trap of using what currently exists (or simply plagiarizing some other company's description from Indeed or another job site). Upon completion of the three circles, you intersect them for your own personal Venn diagram. At the center of the intersection is the unicorn you are looking to hire. Figure 2 provides an example of a Venn diagram for a data scientist. Do not allow this simple diagram to limit your thoughts on skills and capabilities. Three circles are not a limit but are a tool. Be thoughtful; as the number of circles grows, so will your difficulty in acquiring a unicorn. If you begin to find you require more than four circles, chances are you have two different jobs you need to fill.

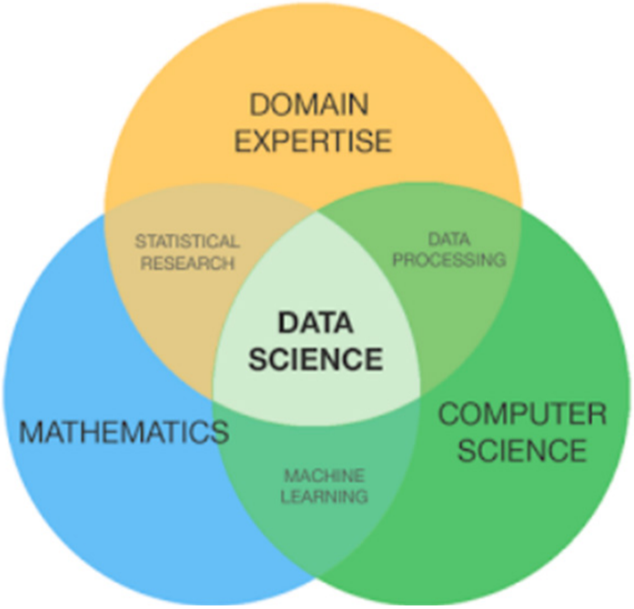


Figure 2. Venn diagram of a data science unicorn.

6. LEVERAGE EXISTING INFRASTRUCTURE OR LOOK INTO NEW INFRASTRUCTURE

By new infrastructure, I do not mean significant capital investment. Remember, this is a journey that will take multiple years. Initially, most companies are using an office suite (e.g., Microsoft, Google, Salesforce, etc.) that they can leverage. If your company currently uses Microsoft, PowerBI is a simple tool that integrates easily for a minimal monthly fee. Don't get caught in the big, expensive solution. Start simple, and as the company begins to reap the benefits of their initial investment, evolution will continue.

How can this be accomplished? First, leadership must break the barriers on access to information and data. Many organizations create significant barriers to accessing data. IT must become a shepherd for sharing data and access. This does not mean being irresponsible with security; it means training and facilitating read-only access to data sources (one-way streets to pull but not write information) and creating data warehouses and data lakes that can be accessed by all (real-time financial information notwithstanding, some information must stay protected to avoid insider trading). Through a combination of access and training using free sources and in-house experts, learning and institutional knowledge will begin to blossom.

7. DEMOCRATIZE YOUR INFORMATION

Democratization of your information – driving the training and tech into all organizational ranks – requires a lot of focus and effort. Through democratization, the exponential growth of knowledge and improvement will rise like a phoenix. There are plenty of free tools available on the web or at edx.org to help with this effort. Heavy dollar investment is not required, only heavy investment in your sweat equity.

Democratization serves two significant purposes. It grows the institutional knowledge and keeps your workforce learning. A business can only grow if its people are growing (learning is the foundation of people growth). Democratization is a form of visual cues that provides a strong and robust safety net capable of seeing information and issues previously unnoticed. Think of it like this: Would fans attend a baseball game if they could not see the score? By driving the information into all ranks, the score is known by all and, more importantly, quality is seen as more than a function; it becomes transformed into an institutional capability embraced by all.

8. AUTOMATE — BUT NOT YET

Many companies want to jump to automation. Avoid this urge. Technology accelerators have their place; however, technology-induced change without proper process or relevancy is a program killer and money pit all in one. People become enamored with the flashing lights and new technological toys. Smart businesses have learned to run, but you must first walk, and to walk you must crawl. The reality is that focusing on finding the right future talent and initial infrastructure and democratizing your information will serve to move your program from a crawl to a walk. Once these elements are going well, you can begin the next phase of leveraging better prediction through automation and machine learning.

Now that you have the right talent, a simple to understand infrastructure, and a well-versed organization, you are primed to use technology to help accelerate good processes and begin to converge with more expansive data sets. Applying the right set of machine learning tools allows a business to create a more informed analysis of existing data for deeper insights and statistical patterns.

Our historical data sets can be used to train algorithms to understand behavioral patterns, anticipate problems, and effectively allow for timely and prepared action. Additionally, these learning algorithms can actively monitor the many different disparate data sources that generate new information daily. Doing so will facilitate the development of early warning signals or, better yet, outline things that are going well. Understanding what works well allows a business to exploit a competitive advantage within its quality program.

Another benefit is that these predictive algorithms can be used to monitor industry trends, including with regulatory agencies and competitive businesses. This monitoring effectively helps you see the winds of change and stay away from oncoming obstacles.

An effective method to determine your automation road map is to evaluate what is working well; this is a candidate to automate and evolve through machine learning. Start with a new set of KPQs and create three circles for your automation Venn diagram. Each circle wraps around an automation concept. For example, what drives customer behaviors around the quality of your products, what issues are your customers passionate about, what type of data exists, and what types of algorithms can be used to explore the data? Combine the three circles into your Venn diagram. The overlap will help shine the spotlight on how to attack and automate your next steps toward an automated predictive program.

CONCLUSION

The FDA's initiative could have significant and costly ramifications for manufacturers, whether in biotechnology, digital health, pharmaceuticals, and anywhere in between. However, by following mDMAP we can mitigate the likelihood of regulatory scrutiny. Starting your mDMAP integration voyage now allows you to stay ahead of the data management curve and protects your business. More importantly, your mDMAP journey will provide greater understanding and help you proactively pivot using the voice of your customers. The proactive capability drives your ultimate goal of doing well by doing good. Or, said another way, we ensure safe and effective outcomes through measured and consistent approaches.

REFERENCE

Vuleta, B. (2021, January 28). How much data is created every Day? [27 POWERFUL Stats]. Retrieved April 02, 2021, from https://seedscientific.com/how-much-data-is-created-every-day/#:~:text=Every%20day%2C%20we%20create%20roughly%202.5%20quintillion%20bytes%20of%20data

ABOUT THE AUTHORS

Matt Collins is a cofounder of Cignyl and serves as its CEO. He brings over 25 years of industry experience with a track record for building consistent and reliable outcomes. He has driven critical turnarounds for complex situations such as warning letters, consent decrees, international regulatory problems, implementation of global systems, network optimizations, and mature business situations. He holds a doctorate in business administration with an emphasis in healthcare and leadership from California Intercontinental University, an MBA from Marquette University, and a BS in molecular biology from the University of Wisconsin Parkside.

John Giantsidis is the president of CyberActa, Inc, a boutique consultancy empowering medical device, digital health, and pharmaceutical companies in their cybersecurity, privacy, data integrity, risk, SaMD regulatory compliance, and commercialization endeavors. He is also a member of the Florida Bar's Committee on Technology and a Cyber Aux with the U.S. Marine Corps. He holds a Bachelor of Science degree from Clark University, a Juris Doctor from the University of New Hampshire, and a Master of Engineering in Cybersecurity Policy and Compliance from The George Washington University.

A LIMS AUDIT FRAMEWORK: WHAT TO AUDIT & HOW TO PREPARE

Dr. Tim Sandle, Ph.D.

Head of Compliance and Risk Management,
Bio Products Laboratory Limited

Laboratory information management systems (LIMS), as well as providing workstream value within the laboratory, are inevitably the subject of regulatory focus and audit. This is due to the criticality of the data and the pivotal role LIMS play in the batch release process. This article considers what to audit and how to audit a LIMS, presenting a framework that will be useful to those planning to undertake a LIMS audit and for laboratory managers who need to prepare for such an audit.

An audit of a LIMS is an examination of the procedures used in a computer system to evaluate their effectiveness and correctness and to recommend improvements. The scope of an audit will vary, and audits of LIMS are often wider for new systems than with established systems that have been subject to multiple audits. In addition, since LIMS will generate data used for batch release, issues relating to the data integrity of batch records will be arguably of greatest concern. Areas to focus on include:[1]

- How the LIMS fits with the quality management system
- Whether the LIMS has been subject to quality risk management
- If a supplier/system vendor audit has been conducted
- The design specification for the LIMS
- The user requirement specification for the LIMS
- The validation procedure for implementing the LIMS, including the approach taken, the validation master plan, and the verification method. The validation plan describes all activities, such as review of the user requirement specification, review of the development plan (design), test strategy, verification of the data migration (if applicable), review of the validation documents, and the acceptance testing of the whole system.
- The change control for the LIMS. All new systems should go through change control, and change control should be used appropriately for existing systems. In the event of changes in the computerized system, including version updates, these should be done first in a test environment, after which the validation status needs to be reestablished. If a revalidation is needed, it should be conducted not just for validation of the individual change, but also to determine the extent and impact of that change on the entire computerized system.

- Configuration management of the LIMS
- Training to use the LIMS

With system validation, the purpose of validation is to confirm that the LIMS specifications conform to the users' needs and intended uses by examination and provision of objective evidence and that the particular requirements can be consistently fulfilled.[2] However, the extent of validation will depend on the complexity and intended use of the computerized system being validated. The validation effort can be scaled and adapted to the type of system, justified by documented risk assessment.

LIMS SUPPLIERS

Prior to purchasing a LIMS, the supplier should be assessed and audited. For the assessment, policies and procedures for the specification, purchase, development, and implementation of computerized systems should ideally be in place. For the audit, a formal extensive review of the history of the supplier and the software package should be undertaken to gain an additional degree of assurance of the reliability of the software. Several international standards can assist with this process. ISO 9001 provides a quality system model for quality assurance in relation to design, development, production, installation, and servicing, where these key principles can be readily applied to computerized systems. In addition, ISO/IEC/IEEE 12207:2017 provides guidance on acceptable practices for information technology – software life cycle processes and ISO 9004, ISO 10005, and ISO 10007 provide guidance on quality management and system elements, including quality plans and configuration management.

Once installed, users should keep detailed records of the performance of the LIMS and address any errors that arise, as well as drawing together any common themes in an annual review. Areas to review for such an overview are the logbook and audit trail.

DOCUMENTS

The organization should have procedures relating to data integrity. These will vary from firm to firm, but may include:

- System maintenance SOP — to ensure that appropriate maintenance is carried out in a controlled way.
- Physical security SOP — for control of secure access (intrusion).
- Logical security SOP — for user and password policy.
- Incident and problem management SOP — to describe how to manage and communicate possible problems.
- System change control SOP — covering areas like how the change may affect the process.
- Disaster recovery SOP — to ensure data protection and recovery of processes.
- Backup and restoration SOP — for the control of regular data backup.

ELECTRONIC RECORDS

A LIMS is designed to produce electronic records. Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. In terms of audit checks, electronic records must contain data and metadata and must be available in a readable format. Furthermore, electronic records must be ready to retrieve during the entire period of retention.

PASSWORDS

Since the LIMS generates digitally signed records that must be controlled according to identification rules, the auditor should assess whether the organization:

- maintains unique passwords and ID codes (usernames)
- ensures periodic password checks/changes are in place
- configures ID privileges individually or on a group basis

- assigns operators, supervisors, and administrators different levels of accessibility
- ensures operators do not have database management rights.

AUDIT TRAILS

Arguably the biggest focus with a LIMS audit is the system's audit trail. The audit trail is data in the form of a logical path linking a sequence of events that is used to trace the transactions that have affected the contents of a record. The computerized system should keep a record of any critical actions that occur, such as, for example, who has accessed it and when, any deletion or change of data, etc. Users must not be allowed to amend or switch off the audit trails or alternative means of providing traceability of user actions.

The auditor should check that audit trails are reviewed by supervisors when results are checked. The review of the audit trail should not only be for the test or activity that has been presented but also for any recent activities that may not have been reported, such as a laboratory technician who has run duplicate tests. The auditor should also assess that the audit trail has been time-stamped. It must record the date and time of operator entries and actions that create, modify, or delete an electronic record.

DATA ENTRY

For some systems, and for many GxP systems, there should be procedures in place for critical data entry. This may require a second check, as determined by risk assessment (such as with the entry of manufacturing formula or the transfer of laboratory data and results from paper records). Where a secondary check is made, this will be by someone with a different login name and identification at a given time and date. Should changes to data entry be required, such corrections must be captured in the audit trail.

With data entry, the system must have defined time zone(s) and date standard referencing with relative transaction linking (it is important to note that complex systems may span several time zones).

ELECTRONIC SIGNATURES

An electronic (or digital) signature is based upon cryptographic methods of originator authentication, computed using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. To be compliant, signed electronic records need to contain:

- The printed name of the signer,
- The date and time when the signature was executed, and
- The action taken (such as review, approval, responsibility, or authorship).

TRAINING

All personnel administering the systems must have appropriate security clearances, training, and skills, together with the necessary knowledge to operate the systems and understand their purpose. Training records should exist for all users of a LIMS, with the records traceable to specific procedures. In relation to training, there should be procedures in place that ensure that entities authorized to use electronic signatures are aware of their responsibilities for actions initiated under their electronic signatures.

ADMINISTRATION

The LIMS should have an appointed administrator. Only the responsible person (this could be designated IT personnel and certainly someone independent of the operation) should have administrative rights to implement any LIMS updates or change critical system settings (such as audit trails or alterations to time/date settings). Such an appointed person should be in place to manage permissions for other users. Other routine tasks, such as for analysis, should be based on user accounts and passwords that do not have administrative rights.

The granting and control of administrative rights should be documented and only be granted to personnel with system maintenance roles that are fully independent of the personnel responsible for the day-to-day use of the system (such as inputting manufacturing data, running laboratory analyses, and so on).

SYSTEM SECURITY

The security of the system and security of the data need to be assessed and the procedures and records pertaining to these aspects should be based on company-wide policies. Examples of areas to assess include:[3]

- Access rights for all operators are clearly defined and controlled, including physical and logical access.
- Different levels of access are assigned to users, including separate management and administrator accounts.
- Each individual using the LIMS should have an individual password, traceable to the individual and known only to the individual and an independent administrator.
- A system is in place for removing users who no longer work for the company.
- Procedures are in place to ensure that identification codes and password issuance are periodically checked, recalled, or revised.
- Loss management procedures exist to electronically invalidate lost, stolen, or potentially compromised passwords.
- The system should be capable of enforcing regular changes of passwords.
- Procedures identify prohibited passwords.
- An audit log of breaches of password security should be kept and measures should be in place to address breaches of password security.
- The system should enforce revoking of access after a specified number of unsuccessful logon attempts.
- Measures are needed to ensure the validated recovery of original information and data following backup, media transfer, transcription, archiving, or system failure.
- Attempted breaches of security safeguards should be recorded and investigated.

SYSTEM BACKUP

There should be a documented and validated backup procedure including storage facilities and media. With this, all GxP related data, including audit trails, should be backed up. The process should assure data integrity. The frequency of backup is dependent on the computer system functions and the risk assessment of a loss of data. Performance of backups should be visible via a review of the audit trail, and a record of rectification of any errors should be kept. Tests should be conducted to show that backed up data is retrievable following a system breakdown.

The routine backing up of data should involve placing the data into a safe storage location, adequately separated from the primary storage location. This could be storage media held in a fireproof safe or on a server. The media used should be documented and justified for reliability.

CONTROL OF COMPUTER SYSTEM ENVIRONMENTS

Computer systems should lock out when not in use and may need to be located in controlled areas. Server rooms should have restricted access and maintain the conditions necessary to ensure the correct functioning of equipment (with control of temperature, firefighting measures, uninterruptible power supply, and so on).

5-STEP APPROACH

- One way to conduct a LIMS audit is to adopt the five-step approach.[4] These are:
- Conduct the initial review (planning the audit).
- Review and assess internal controls.
- Conduct compliance testing (test the internal controls).
- Perform substantive testing (test the detailed data).
- Reports (conclusions and findings).

The auditor(s) should reach an understanding with the client concerning the scope and limitations of the audit from the very beginning. This will facilitate accomplishment of the audit objectives in an effective and efficient manner. As part of audit preparation, the auditor should conduct a preliminary survey of the entity to plan how the audit should be conducted. The auditors gather information about the LIMS that is relevant to the audit plan, including: a preliminary understanding of how the LIMS' functions are organized; identification of the computer hardware and software used by the entity; a preliminary understanding of each significant accounting application processed by computer; and identification of planned implementation of new applications or revisions to existing applications and applicable controls.

With LIMS there are two types of controls: general and application. General controls are those that cover the organization, management, and processing within the computer environment but are not tied to particular applications. They should be tested prior to application controls because if they are found to be ineffective the auditor will not be able to rely on application controls. General controls include such things as proper segregation of duties, disaster plan, file backup, use of labels, access control, procedures for acquiring and implementing new programs and equipment, and so on. Application controls relate to specific tasks performed by the system. They include input controls, processing controls, and output controls and should provide reasonable assurance that the initiating, recording, processing, and reporting of data are properly performed.

The system owner should perform compliance testing to determine whether the controls actually exist and function as intended. There are three general approaches to compliance testing: the test data approach, taking a laboratory example, where the auditor has test results processed through the client's system and then compares the results to predetermined results; the integrated test facility approach, where dummy test results are processed along with real test results and compared to auditors' predetermined results; and the parallel simulation approach, in which real test results are processed through the client's system and also through a parallel system set up by the auditor using the same programs, and the results are compared. Whichever of these test approaches is used, the results should tell the auditor if the controls exist and are functioning properly.

SIGNIFICANT NON-COMPLIANCES

Although the auditor may pick up on several areas of concern, arguably the most significant issues that an auditor could find are:

- The lack of a written detailed description of each system
- System log not kept up to date with controls over changes
- Weak security in place
- No audit trails in place or audit trails not active
- Lack of evidence for the quality assurance of the software development process
- Inadequate validation of the LIMS
- Improper data manipulation
- Adjustment of time clocks
- Backdating of information
- Creating records after the fact or without actually executing the procedure
- Excluding adverse information
- Sharing of passwords
- Discarding or destroying original records

The above list feeds into the area of data integrity. Preventing data integrity breaches can be addressed with three primary elements: personnel and training, good system validation, and maintaining security.

SUMMARY

This article provides a framework for conducting a LIMS audit, providing advice for both the auditor and auditee. Focal points within the audit process include verifying how well LIMS handles electronic data exchanges, how an instrument's input and output data are managed, and how reliable the outputs are in terms of batch reports and trend reports.

This article has been adapted from chapter 2 of the book Digital Transformation and Regulatory Considerations for Biopharmaceutical and Healthcare Manufacturers, Volume 2, written by Tim Sandle and co-published by PDA and DHI. Copyright 2021. All rights reserved.

REFERENCES

1. PDA (1999) Validation and Qualification of Computerized Laboratory Data Acquisition Systems, Parenteral Drug Association, Technical Report #18, Bethesda, MD, USA

2. Wingate, G. (1997) Validating Automated Manufacturing and Laboratory Applications: Putting Principles into Practice, Taylor and Francis, New York, USA, pp10-15

3. Skobelev, D.O., Zaytseva, T.M., Kozlov, A.D., Perepelitsa, V.L. and Makarova A. S. (2011). Laboratory information management systems in the work of the analytic laboratory. Measurement Techniques. 53 (10): 1182–1189

4. Conti, T.J. (1992) LIMS and quality audits of a quality control laboratory. Chemometrics and Intelligent Laboratory Systems, Laboratory Information Management, 17: 301–304

ABOUT THE AUTHOR

Tim Sandle, Ph.D., is a pharmaceutical professional with wide experience in microbiology and quality assurance. He is the author of more than 30 books relating to pharmaceuticals, healthcare, and life sciences, as well as over 170 peer-reviewed papers and some 500 technical articles. Sandle has presented at over 200 events and he currently works at Bio Products Laboratory Ltd. (BPL), and he is a visiting professor at the University of Manchester and University College London, as well as a consultant to the pharmaceutical industry. Visit his microbiology website at https://www.pharmamicroresources.com.

IMPORTANT CGMP CONSIDERATIONS FOR IMPLEMENTING ELECTRONIC BATCH RECORDS

Dr. Tim Sandle, Ph.D.

Head of Compliance and Risk Management,
Bio Products Laboratory Limited

While human error is never the ultimate root cause, mistakes in batch records can have considerable consequences for the release of medicines in terms of delays and rejections. In more serious cases, when the error is initially undetected, the consequence can be a product recall. Errors can be minimized through the implementation of electronic batch records. However, with any electronic system within the pharmaceutical industry, the requirements of current good manufacturing practice (cGMP), including those of data integrity, need to be met. These essential requirements need to be included in the initial design phase of the system.

CGMP FACTORS FOR SUCCESSFUL ELECTRONIC BATCH RECORDS

A central part of cGMP concerns electronic data management, not least because control of the use of batch records when manufacturing pharmaceutical and biotechnology products is regulated to assure product quality and patient safety. cGMP in relation to electronic records includes:

- limiting system access to authorized individuals
- use of operational system checks
- use of authority checks
- use of device checks
- determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- appropriate controls over systems documentation

These requirements need to also be considered for all electronic records, with specific attention to electronic batch records. The electronic batch record uses the certified copy of the Master Batch Record in the form of a digital document with a digital signature. Through the data capture process, data is compiled and aggregated. The management of the validation and traceability of the data is a cGMP concern, requiring aspects like electronic signatures to confirm each operation and to electronically recognize each operator.

A driver of the adoption of electronic batch records is reduction of errors. One study found a 75% decrease in human errors in electronic batch records compared to a hardcopy system, thereby yielding improvements in production efficiency. The main disadvantages were cost, implementation resources, and the in-built obsolescence of manufacturing software systems. Despite these disadvantages, the study found that implementation of an electronic batch record system resulted in a significant increase in production efficiency.[1]

Yet, electronic batch records need to be implemented according to cGMP if they are to successfully deliver error reduction and avoid flaws in design that might lead to error creation. Guidance on electronic records is provided by 21 CFR Part 11, Electronic Records, Electronic Signatures; ISO/IEC 17799114; The Good Automated Manufacturing Practice Guide for Validation of Automated Systems in Pharmaceutical Manufacture; and FDA guidance documents on 21 CFR Part 11.[2] The CFR requires:

- The ability to determine the existence of invalid or altered records.
- System access is limited to authorized individuals.
- There is a secure, computer-generated, time-stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records.
- Operational systems checks exist that enforce permitted sequencing of steps and/or events as appropriate.
- The identity of an individual is verified before the individual's electronic signature, or any element of such electronic signature, is established, assigned, certified, or otherwise sanctioned.
- Transaction safeguards are used to prevent unauthorized use of passwords and/or identification codes and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

These principles should tally with an organization's data governance process and should be checked at each stage of electronic batch record design and implementation.

Given that the connection of sensors and equipment is important for capturing batch data in real time, data acquisition must not be overlooked. The FDA guidance also covers batch SCADA (supervisory control and data acquisition) systems. Where data can be captured electronically, the following are possible:

Enhanced validation to ensure functionality creates compliant electronic records and signatures

- Enhanced SOPs for life cycle management
- Limited system access by authorized individuals to CPU and data files with automated identity verification with electronic signature and electronic logging of recipe procedures executed by system with time-stamped audit trails
- Protection of records to maintain data integrity and enable retrieval
- Non-obscured revisions to electronic data records with traceable version histories

Where the above requirements are met, the importance of SCADA systems is automation. A SCADA system enables manufacturers to:

- Produce multiple products periodically using the same equipment
- Produce products requiring a multitude of different recipes of ingredients and equipment operations
- Associate each batch with different production orders targeted for different containers, customers, and locations
- Develop production schedules that account for numerous factors such as specific customer orders, quantity, materials, equipment, logistics, shelf-life, and setup time
- Store production data recorded during batch execution in a manner such that it is directly associated with a specific batch production run identifier

The technology allows an organization to carefully study and anticipate the optimal response to measured conditions and execute those responses automatically every time. Relying on precise machine control for monitoring equipment and processes can eliminate most human error. This goes some way to meeting cGMP expectations. Another step is with a thorough consideration of data integrity.

DATA INTEGRITY

There are some specific data integrity requirement pertaining to electronic records, including, in particular, for storage and backup. To recap, data integrity is defined as the extent to which all data are complete, consistent, and accurate throughout the data's life cycle.

Data must be stored and backed up securely, utilizing a validated process and controlled by verification of completeness. Where data retention is outsourced to an external party, the elements of the contract that relate to ownership and retrieval of data should be thoroughly understood, and the vendor should be qualified and managed like any other critical services vendor through established vendor management processes.

Further, with electronic records, the relevance of data retained in audit trails should be considered by each organization in order to permit robust data review. An audit trail is a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the events relating to the creation, modification, or deletion of an electronic record.[3]

Electronic records should be assessed for compliance with data integrity standards. The following checklist may prove useful in this regard:[4]

- How is data collected and reported?
- How is data reviewed?
- How is the integrity of data protected?
- How are calculation errors handled?
- How are alarms managed?
- Who has the authority to invalidate data?
- What happens to this data? (For instance, is it discarded or archived with sample analysis package?)
- How is electronic data protected from editing, changing, deletion?
- How are passwords assigned and protected?

To mitigate risks stemming from the above, each organization operating electronic batch records should have:[5]

- An understanding of computerized system capabilities and transfer of data between systems.
- An up-to-date listing of all relevant systems and GMP functionality.
- Control of networked and stand-alone instruments.
- Policies and procedures detailing processing and control of data.
- Policies and procedures regarding security of the system and user access levels, including appropriate segregation of duties.
- Policies and procedures for electronic signatures, including use of individual and generic passwords.

Overall, all data captured within the electronic batch record must be attributable, legible, contemporaneous, original, and accurate.

These design principles help to drive error reduction, although attention also needs to be paid to staff training to ensure acceptance of a different way of working. Digital transformation is as much about the technology as it is about corporate leadership and redesigning workplace culture.

SUMMARY

Bringing together various processes and laboratory databases that hold the data recorded during manufacture of a batch in a digital format is becoming more common. Electronic batch records can present a more streamlined and less error-prone means to assess and release pharmaceuticals, provided the design is appropriate and that cGMP principles have been adhered to. Of the important aspects of GMP, ensuring that the data captured are reliable and accurate is essential; hence, data integrity considerations need to be at the forefront of any electronic batch record implementation exercise and part of the everyday use of such systems.

This article has been adapted from chapter 8 of the book Digital Transformation and Regulatory Considerations for Biopharmaceutical and Healthcare Manufacturers, Volume 1, written by Tim Sandle and co-published by PDA and DHI. Copyright 2021. All rights reserved.

REFERENCES

1. Marsh, J. L. and Eyers, D. R. (2016) Increasing Production Efficiency Through Electronic Batch Record Systems: A Case Study. In: Setchi R., Howlett R., Liu Y., Theobald P. (eds) Sustainable Design and Manufacturing 2016. SDM 2016. Smart Innovation, Systems and Technologies, vol 52. Springer, Cham, pp261-269

2. FDA (1997) 21 CFR Part 11, Electronic Batch Records, 62 Federal Register 13464, Mar. 20, 1997, US Food and Drug Administration

3. Schmitt, S. (2014a) Data Integrity, Pharmaceutical Technology Europe, 38 (7). Online edition: http://www.pharmtech.com/data-integrity

4. Sandle, T. and Sandle, J. (2019) Audit and Control for Healthcare Manufacturers: A Systems-Based Approach, PDA / DHI Books, River Grove, IL, USA

5. Schmitt, S. (2014b) Data Integrity - FDA and Global Regulatory Guidance, Journal of Validation Compliance, 20 (3). At: http://www.ivtnetwork.com/article/data-integrity-fda-and-global-regulatory-guidance

ABOUT THE AUTHOR

Tim Sandle, Ph.D., is a pharmaceutical professional with wide experience in microbiology and quality assurance. He is the author of more than 30 books relating to pharmaceuticals, healthcare, and life sciences, as well as over 170 peer-reviewed papers and some 500 technical articles. Sandle has presented at over 200 events and he currently works at Bio Products Laboratory Ltd. (BPL), and he is a visiting professor at the University of Manchester and University College London, as well as a consultant to the pharmaceutical industry. Visit his microbiology website at https://www.pharmamicroresources.com.

COMPLYING WITH BATCH RELEASE: AUDITING ELECTRONIC BATCH RECORDS

Dr. Tim Sandle, Ph.D.

Head of Compliance and Risk Management,
Bio Products Laboratory Limited

To ensure that quality is maintained throughout the pharmaceutical or healthcare organization, frequent audits, both internal and external, are required to assess the quality and effectiveness of the processes, systems, and personnel employed by the company. Audits are an important part of quality assurance and the quality management system. This concept needs to apply to computerized systems as much as physical operations. Within pharmaceuticals, perhaps the most important computerized system is the electronic batch record.

This article presents some advice for auditing electronic batch records to assess their current good manufacturing practice (cGMP) status. This is useful in the qualification stage and essential once the electronic record system is in operation. It is only through conducting rigorous audits that the pharmaceutical organization can stay ahead of the regulatory expectations.

ELECTRONIC BATCH RECORDS AND THE AUDIT PROCESS

As computerized systems, electronic batch records should be subject to audit to verify that systems and applications are appropriate, efficient, and adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity. There are different approaches that can be taken to such audits and different types of internal audits, including the following:

- Verification audit
- Annual audit
- For cause audit (such as arising from quality management system reviews, CAPAs, change control, data migration)
- In response to regulatory trends
- Following the acquisition of a new computerized system.

In addition, the organization will often opt to audit a vendor, especially when purchasing a new computerized system.[1] Such an audit may also arise if issues develop with a given system.

There will also be audits of the organization by a standards body or regulatory agency.

- Audits often begin by reviewing the system inventory. This can include:
- Identification of the system and versions
- Purpose of the system
- Validation status
- Physical or storage (drive and files path) location of the computerized system and related documentation
- The name of the responsible or contact person.

Validation will include an assessment of areas like structural integrity, operational reliability, and ongoing support for the software and hardware products used in the electronic batch records system.

Areas to focus on include:[2]

- How the computerized system fits with the quality management system
- Whether the computerized system has been subject to quality risk management
- Whether a supplier/system vendor audit has been conducted
- The design specification for the computerized system
- The user requirement specification for the computerized system
- The validation procedure for implementing the computerized system. This will include the approach taken, the validation master plan, and the verification method. The validation plan describes all activities, such as review of the user requirement specification, review of the development plan (design), test strategy, verification of the data migration (if applicable), review of the validation documents, and the acceptance testing of the whole system.
- The change control for the computerized system. All new systems should go through change control, and change control should be used appropriately for existing systems. In the event of changes in the computerized system, including version updates, these should be done first in a test environment, after which the validation status needs to be re-established. If a revalidation is needed, it should be conducted not just for validation of the individual change but also to determine the extent and impact of that change on the entire computerized system.
- Configuration management of the computerized system
- Training to use the computerized system

Fundamental to the audit process is the accumulation of evidence. During an audit, the auditor will be seeking to establish that the process under review is as it is expected to be and for this, they will require audit evidence. For this to happen, the auditor will be assessing what they are told, hear, and see to determine if it complies with the audit criteria.

The most significant issues that an auditor could find are:[3]

- The lack of a written detailed description of each system.
- System log not kept up to date with controls over changes.
- Weak security in place.
- No audit trails in place or audit trails not active.
- Lack of evidence for the quality assurance of the software development process.
- Inadequate validation of the computerized system.
- Improper data manipulation.
- Adjustment of time clocks.
- Backdating of information.
- Creating records after the fact or without actually executing the procedure.
- Excluding adverse information.
- Sharing of passwords.
- Discarding or destroying original records.

DATA INTEGRITY

The above list feeds into the area of data integrity. Preventing data integrity breaches can be addressed with three primary elements: personnel and training, good system validation, and the maintenance of security.

Data integrity can be subdivided into two distinct areas:[4]

- Physical integrity, which is concerned with the challenges associated with correctly storing and fetching the data itself.
- Logical integrity, which focuses upon the correctness or rationality of a piece of data, given a particular context.

Beneath this there are various subtypes, such as referential integrity, which refers to the database rule that a primary key cannot be duplicated in a table. This also ensures that if the primary key in one table is changed, then the foreign keys in the other tables are also updated.

For computerized systems, good data integrity practices need to be considered in the design, implementation, and use of any system that stores, processes, or retrieves data. With databases, for example, data retention is an important aspect of data integrity, such as specifying the length of time data can be retained in a particular database.

In pharmaceuticals and healthcare, data integrity is fundamental to a pharmaceutical quality system that ensures that medicines are of the required quality.[5] Inadequate data integrity systems could open an organization to risks of recalls and defective product, potentially resulting in:

- Patient death, chronic illness, or disability.
- Regulatory statements of non-compliance.
- Importation ban(s).
- Loss of consumer and regulator trust/confidence, which is exceedingly difficult to recover.
- Product application reviews suspended.
- Market and share price reduction.

Each of the above indicates that data integrity is a particularly important issue that organizations need to be aware of, risk assess, and have measures in place to meet regulatory expectations.

Following the audit process, each organization should undertake a risk review and take action accordingly, beginning with those items identified as being of the greatest risk.

SUMMARY

Computerized systems, including electronic batch records, matter greatly for the modern healthcare or pharmaceutical facility, and more manufacturing processes and data collection operations are being automated. While many software designers are employing good development and documentation practices, followed by robust validation and verification activities before releasing their products, this cannot be assumed. This necessitates the need to audit the design process and to undertake robust computerized system validation. In addition, the day-to-day practices of operating electronic batch records also needs to be periodically audited as part of the quality system to ensure that the required controls are in place and that important control features (such as passwords) and verification steps (such as assessing audit trails) are in place. The essential elements of a compliant electronic batch record system can perhaps be summed up as:

- Ensure that only validated and secure computerized systems are used.
- Ensure access by authorized personnel only.
- Require the use of passwords and access controls to ensure that people have access only to functionality that is appropriate for their job role and that actions are attributable to a specific individual.
- Create backup copies and check the integrity and accuracy of backup data and the ability to restore the data during validation, and monitor this periodically.
- Ensure independent checking of critical data.
- Have procedures in place for the safe storage of data for the required time. The routine backing up of data should involve the placing of the data into a safe storage location, adequately separated from the primary

storage location. This could be storage media held in a fireproof safe or onto a second server.

- Incorporate procedures for the systematic use of an accurate and secure audit trail. The items included in the audit trail should be those of relevance to permit reconstruction of the process or activity.

The above list forms part of data integrity expectations, where data must be attributable, legible (permanent), contemporaneous, original, and accurate. These concerns need to be considered across the product life cycle, as captured by the electronic batch record. The data life cycle considers all phases in the life of the data, from initial generation and recording through processing, use, archiving, retrieval, and (where appropriate) destruction. Failure to address just one element of the data life cycle will weaken the effectiveness of the measures implemented elsewhere in the system. This is why auditing electronic batch records is a compliance necessity.

Tim Sandle's new book, *Digital Transformation and Regulatory Considerations for Biopharmaceutical and Healthcare Manufacturers, Volume 1: Digital Technologies for Automation and Process Improvement*, has been published by DHI and is available via the PDA Bookstore: https://www.pda.org/bookstore/product-detail/5897-digital-transformation-volume-1.

REFERENCES

1. Stembridge, K. and Adkins, M. (2018) Making the Move to Electronic Batch Records, Pharmaceutical Technology, 42 (4): 52-55

2. PDA (1999) Validation and Qualification of Computerized Laboratory Data Acquisition Systems, Parenteral Drug Association, Technical Report #18, Bethesda, MD, USA

3. Sandle, T. and Sandle, J. (2019) Audit and Control for Healthcare Manufacturers: A Systems-Based Approach, PDA / DHI Books, River Grove, IL, USA

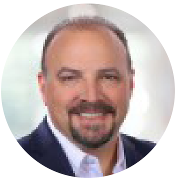
4. Sandle, T. (2016) Risk Assessment and Management for Healthcare Manufacturing: Practical Tips and Case Studies, PDA / DHI, Bethesda, MD, USA.

5. FDA (2018) Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry, December 2018, U.S. Department of Health and Human Services, Food and Drug Administration, Washington

ABOUT THE AUTHOR

Tim Sandle, Ph.D., is a pharmaceutical professional with wide experience in microbiology and quality assurance. He is the author of more than 30 books relating to pharmaceuticals, healthcare, and life sciences, as well as over 170 peer-reviewed papers and some 500 technical articles. Sandle has presented at over 200 events and he currently works at Bio Products Laboratory Ltd. (BPL), and he is a visiting professor at the University of Manchester and University College London, as well as a consultant to the pharmaceutical industry. Visit his microbiology website at https://www.pharmamicroresources.com.

DATA INTEGRITY IN SUPPLY CHAIN RISK MANAGEMENT DURING ZERO TRUST



Kip Wolf

Head of Technical Operations and Portfolio Management, X-Vax Technology, Inc.

Our lives have changed so very much because of the global pandemic. Many have personally and professionally suffered, and many economies and businesses are forever changed. We also have been and continue to be impacted by supply chain constraints from both direct and indirect consequences of the global pandemic. Regardless of industry segment or stage of product life cycle, this phenomenon has required us to reconsider our approaches to supply chain risk management and to develop new and creative risk management strategies and tactics in response.

A CALL TO ACTION

Ironically, April 2021 marked the fourth annual National Supply Chain Integrity Month in the United States, where the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), and other government and industry partners work to promote "a call to action for a unified effort by organizations across the country to strengthen global supply chains."[1]

The U.S. National Counterintelligence and Security Center (NCSC), one of the centers coordinated under the Office of the Director of National Intelligence, "works with its partners to assess and mitigate the activities of foreign intelligence entities and other adversaries who attempt to compromise the supply chains of our government and industry."[2] The NCSC produced and published in 1Q2021 a summary document of *Best Practices for Supply Chain Risk Management* that includes a call to action, with recommended activities grouped into summary tasks as shown below:[3]

- Obtain executive level commitment for a supply chain risk management (SCRM) program.
  - Build an integrated enterprise team.
  - Communicate across the organization.
  - Establish training and awareness programs.

- Identify critical systems, networks, and information.
  - Exercise asset management.
  - Prioritize critical systems, networks, and information.
  - Employ migration tools.
- Manage third party risk.
  - Conduct due diligence.
  - Incorporate SCRM requirements into contracts.
  - Monitor compliance.

The need for SCRM program sponsorship and support is now almost universally understood. And the identification and management of critical systems, networks, and information is commonplace. What we have learned from the recent pandemic is that the third-party risks require additional diligence, particularly about data integrity. The table below provides some context and a framework to help understand the shift in risk profile and data integrity focus learned from our experiences during the recent global pandemic. Two key lessons are summarized here by way of considering two pairs of ALCOA principles: Contemporaneous and Accurate and Attributable and Original.

Table 1: List of ALCOA principles and related data expectations.

Principle	**Data Expectations**
Attributable	• Clear identification of the system or individual that created or modified the data.
Legible	• Permanence and readability of original data (for duration of the data life cycle).
Contemporaneous	• Data recorded at the time of activity or event.
Original	• First instantiation of the data (electronically or otherwise) as supported by evidence.
Accurate	• Without error.

LESSON 1: CONSIDER HOW THE PRINCIPLES OF "CONTEMPORANEOUS" & "ACCURATE" AFFECT SCHEDULING

The first SCRM lesson we learned from the pandemic was that the information provided by suppliers was not accurate, if it was provided at all. Risks related to logistics and visibility of timing of shipments are greater when the accuracy of the data provided by suppliers is suspect. In the pre-pandemic times, supplier estimates were rather reliable. We were accustomed to having direct visibility of the detailed order status. We could track in near real time from order to fulfillment to shipment to receipt. However, as the pandemic developed, these data became less and less accurate as data entry also became less and less contemporaneous. Statuses along the supply chain began to languish and lack updates. Suppliers became overwhelmed with calls and emails requesting updates on orders, until, finally, they stopped responding. Shipment status went from "ordered" to an estimated time of arrival (ETA), to delayed ETA, to greatly protracted date estimates (e.g., "late 2022"), to "no ETA," or even no response at all. We literally found ourselves at the mercy of the delivery service, waiting with anxiety to see what would show up each day.

In the end, the errors, inaccuracies, and delays in data reporting led to lagging indications of supply chain issues and failures from having to react to lost shipments. Global carriers were not immune from these types of catastrophic failures. We heard of shipments vanishing without a trace, from lost components and materials to larger volumes of drug substance just disappearing during transit without explanation. The material impact is quantifiable. The public health impact of delays in access to therapies may be immeasurable.

As a result, there is now greater focus on the accuracy and timeliness (i.e., contemporaneousness) of supply chain status data. Greater attention is paid to the supporting systems such as utilities and internet service to ensure uptime to prevent delay or loss of supply chain data capture and reporting. Greater effort is made in qualification or requalification of suppliers to ensure not only conformance to regulatory requirements but to ensure that capabilities exist to support more stringently defined supply requirements. To simply demand increased visibility and transparency is ineffective. Instead, a clear definition of data requirements and information sharing tactics is necessary for transformational change. Changes in supply chain management of risk will occur over time, but only if we are diligent about transforming the processes and remain vigilant about data integrity along the way.

LESSON 2: CONSIDER HOW THE PRINCIPLES OF "ATTRIBUTABLE" & "ORIGINAL" MAY HELP PREVENT COUNTERFEIT & FRAUD

The second SCRM lesson we learned from the pandemic made us somewhat pessimistic. There was a great shift in economies, markets, and business opportunities. We watched as some industries suffered and may never return to pre-pandemic conditions (e.g., restaurants), while other markets expanded, not all of them legitimately.

A great rise in hoarding of materials and black-market economies placed additional strain on an already suffering global supply chain. Counterfeit materials, intermediates, and products have had economic and public health or safety implications. Blatant fraud has delayed medical services or even cost lives. We have seen large organizations and enterprises pay six or even seven figures for gloves and other personal protective equipment (PPE) that when delivered turned out to be non-sterile or not as advertised. Worse, some buyers found that the warehouses and trucks for which they paid dearly for PPE were in fact empty! Yes, this blatant fraud continues to occur, with no opportunities for recourse or restitution.

Again, data integrity principles may be part of the ultimate solution. We must demand verification of data to confirm attribution and originality. Change the ordering and acceptance criteria to include confirmation of metadata and evidence to check and double-check the authenticity of the data on which key supply chain decisions are made. And expand the scope and scale of verification beyond the immediate supplier to secondary and tertiary suppliers (e.g., to intermediates, components, or raw materials). Demand data provenance for key supply chain information both in electronic system-generated data and in human-created paper records.

A TIME FOR DATA TRANSFORMATION

We must change the way we operate as individuals, organizations, corporations, and nations in this period of limited or zero trust. This is a realistic vision, not a pessimistic view. We must change the way we manage supply chain risk both quantitatively and qualitatively. We must increase quantitatively our reassessment of the risk profile(s) to perform them as often as necessary, even daily, when threats are present. We must improve qualitatively the methods employed for both supplier qualification and supply chain management, ensuring that we are probing both deep and wide into the data and metadata associated with the supply relationships and related transactions.

Transformational change is upon us. Like the tamper-resistant packaging that we are all so accustomed to because of the Tylenol murders and industry response in 1982, our supply chain risk management strategies will forever be altered by the COVID-19 pandemic to demand robust data in near real time that is fully verified through confirmation of data integrity.

REFERENCES

1. "Supply Chain Integrity Month | CISA." Accessed May 24, 2021. https://www.cisa.gov/supply-chain-integrity-month.
2. "Supply Chain Threats." Accessed May 24, 2021. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats.
3. National Counterintelligence and Security Center (NCSC). "Supply Chain Risk Management: Best Practices in One Page – 2021," 1Q2021. https://www.dni.gov/files/NCSC/documents/supplychain/SC_Best_Practices_Final_2021.pdf.

ABOUT THE AUTHOR

KipKip Wolf is head of technical operations and portfolio management at X-Vax Technology, Inc. His technical experience includes the fields of quality assurance and regulatory affairs, GMP and IT compliance, technical operations, and product supply. His areas of leadership expertise include business transformation, new business development, organizational change leadership, and program/project management. He has led business process management groups at Wyeth Manufacturing and at Merck Research & Development. Prior to joining X-VAX, he supported the company as a principal consultant at Tunnell Life Sciences Consulting, where he also led the data integrity practice.

9 PITFALLS TO AVOID IN DATA INTEGRITY IN PHARMACEUTICAL AND DEVICE DEVELOPMENT & OPERATIONS

Peter H. Calcott, Ph.D.
President & CEO, Calcott Consulting LLC

In the first article of this two-part series, I shared five common misconceptions in data integrity (DI). In this article, I will illustrate with examples areas where I have seen significant DI implementation problems in companies I have worked with. This should not be viewed as an exhaustive listing but rather those I have found that illustrate the diversity of issues.

1. PART 11 COMPLIANCE

Part 11 compliance has been around for about 20 years,[1] but still today I see confusion in the industry. While most elements have been implemented successfully, in part attributable to the array of great software available in the marketplace, there are still areas where people stumble. I will illustrate two areas.

First, while almost all my clients purchase software in the marketplace, the systems fall into two types for the purpose of this point. The systems that reside in the cloud, where you access the application via the internet, usually are very robust. However, I have seen clients disable certain features that can have impact (e.g., audit trails). On e-systems that reside on a PC at the site of use, I have witnessed several problematic incidents. These all focus on the integrity of the clock used to date-stamp data. In these examples, the software has used the Microsoft (computer) clock to date-stamp the data rather than the software clock. In both cases, the Microsoft clock was not protected, and I could change the date and time with a click of the mouse. This rendered the date stamp worthless. The simple fix was for the administrator to lock the computer setting so that analysts could not change it. Of course, the system administrator can still do that.

Second, assignment of appropriate access based on job function is critical for meeting Part 11 compliance. At larger companies, there are at least three levels of access, easily recognizable. I will use setting up access levels for a High Pressure Liquid Chromatography (HPLC) as an example. The most restrictive is for staff who simply review data, either rejecting or approving the results. This is common for supervisors or manager-level staff. The next level is assigned to analysts, where they need to be able to set up runs, review data, and make adjustments to, for instance, integration parameters. And finally, there is the system administrator, who has complete access to the inner

working of the system. In some smaller companies, these assignments are often blurred, with "super users" having administrator rights although they actually run samples and process data. This means that these analysts can actually access the file systems and make major adjustments. This leads to situations where DI can be questioned. It is particularly important to assign the access based on job function and separate the administrative functions from analyst roles. This tends to be a problem particularly in smaller companies.

2. INTEGRATION OF HPLC CHROMATOGRAMS

Ideally, software should be set up to run automatically and integrate correctly every time. However, in many analyses, integration is not perfect, requiring post-analysis adjustments. If this is the case, it is paramount to incorporate into the method SOP a procedure to follow, with appropriate documentation, so the reintegration is performed in a reproducible compliant and documented manner. Without these controls and checks, it leaves the company open to DI questions.

3. OUT OF SPECIFICATION (OOS) INVESTIGATIONS

Even after the "Barr Case" of 1993,[2] companies run into problems with how they conduct OOS investigations. There needs to be a robust SOP detailing how you proceed when a suspected OOS is encountered. Initially, before any investigation into product quality, there needs to be an assessment as to whether the method was run correctly in the laboratory. If an error can be demonstrated, the whole result or even the whole run can be nullified and the run or sample repeated. Once the run is shown valid, or at least cannot be nullified, then a product investigation can be considered. A detailed investigation plan, including repeat testing or retesting, must be drawn up and executed. Failure to follow a structured plan can create doubt about your DI status and conclusions.

4. ENVIRONMENTAL MONITORING (EM) DATA

Particularly in sterile or aseptic processing operations, many EM data are generated and analyzed. Obviously, the correlation between numbers of colonies on plates and the results on test forms must be perfect. So, when I routinely audit operations, I often review these forms. Even well-run operations will pick up counts on plates quite normally. If I see page upon page of zero colony forming units, my suspicions are triggered. If it looks too good to be true, it usually is.

5. REPORTS THAT DE-EMPHASIZE DATA THAT COMPROMISES THE STUDY – VALIDATION AND INVESTIGATIONS

As I indicated in part 1 of this article series, any discrepancy or deviation or anomalous data that is generated in an investigation or validation must be considered in the context of the end result of the report. Too many times, I have found results that might cast doubt on a conclusion are ignored and not discussed. Not all "failing" results or deviations will necessarily nullify the conclusion. In many cases, other tests can be performed to address the anomaly. At the end of the day, you want a report that can be read by others (including an inspector) that is correct and convincing.

6. CHERRY-PICKING DATA

In many MHRA and FDA presentations and guidances,[3-7] they have described cherry-picking of data. That is the tendency to keep testing until you get the result you "want" – usually a passing result. It often manifests in using unofficial databases to house data, running trial samples, using test samples to "calibrate" systems, and the list goes on. In the GMP world of validated methods, you get a chance to run a sample once according to the SOP. Only if you can prove there was a lab error can you justify nullifying the test and repeating it. While FDA warning letters are rife with incidents, I have found in auditing it often happens in smaller companies that are transitioning from being solely a research company to a development company moving into clinical trial manufacturing. Often, the senior staff is research trained and not familiar with the GMP requirements. It is a hard transition to make in a career. I know because I made that transition a long time ago.

7. MAKING DATA AND SAMPLING PORTS ACCESSIBLE

Although I have never seen an example of this in my years of auditing, I am including it because the MHRA used this example in its 2018 guidance[6]. By this, they mean that a sampler might be tempted to sample not from the correct port in, for instance, a WFI loop, but rather another from a more accessible one, if the former is difficult to get to. So, we must be vigilant to assure we do not install obstacles in the way of our staff getting their jobs done correctly.

8. QA-ISSUED FORMS

Any blank form used in your operations (on the shop floor or QC labs) must be a controlled form. That is, it must be QA issued (appropriately reviewed and approved) *and* be issued with a unique identifier. QA needs to keep an inventory of those issued, when, and to whom. If the forms are available online and can be printed off by an operator, then the control is lost. A form can be filled in or destroyed with no record. I have found this is a difficult principle for some smaller companies to grasp. If you do not track issuance of your forms, you are open to questions about the integrity of your documentation.

9. TRANSITIONING FROM RESEARCH TO REGULATED ENVIRONMENT

I have found that the transition from a completely research organization to a development and commercial organization can be problematic in this area. Researchers are used to experiments not working, resulting in their repeating the process until it works. It is part of the research method. So, when those staffers transition over to a more regulated operation, for instance during clinical manufacturing, that transition can be very traumatic. Many actions acceptable in research are just not compliant to the GMP regulations. This is particularly true in DI, illustrated in some of the areas above.

DI is a hot topic with regulators at the present time. There are good guidances out there to help and educate you.[3-9] What is most important is to recognize that DI issues can affect any person or organization. I would encourage all to consider that it might actually be happening in your organization as you read this article. Do not wait for the regulators to discover it in your operation. Rather, be proactive and seek out assurances that it is not occurring in your operations. With the intelligent use of ICH Q9 – Quality Risk Management[10] techniques, you can systematically assess your processes, identify weaknesses, and remedy them before you have a data integrity crisis on your hands.

REFERENCES

1. 21 CFR Part 11 Electronic Records; Electronic Signatures — Scope and Application
2. United States v. Barr Laboratories, Inc., 812 F. Supp. 458 (D.N.J. 1993) https://law.justia.com/cases/federal/district-courts/FSupp/812/458/1762275/
3. MHRA GMP Data Integrity Definitions and Guidance to Industry March 2015
4. FDA Data Integrity and Compliance with GMP April 2016
5. EMA Data Integrity August 2016
6. MHRA "GX" Data Integrity Guidance and Definitions March 2018
7. FDA Data Integrity and Compliance with Drug CGMP December 2018
8. PIC/S Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments August 2016
9. WHO Technical Report Series Number 996 2016
10. ICH Q9 Quality Risk Management
11. PIC/S Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments July 2021

ABOUT THE AUTHOR

Peter H. Calcott, D.Phil., is president and CEO of Calcott Consulting LLC, which delivers solutions to pharmaceutical and biotechnology companies in the areas of corporate strategy, supply chain, quality, clinical development, regulatory affairs, corporate compliance, and enterprise e-solutions. He has also served as an expert witness. He also teaches at the University of California, Berkeley in the biotechnology and pharmaceutics postgraduate programs. Previously, he was executive VP at PDL BioPharma, chief quality officer at Chiron and Immunex Corporations, and director of quality assurance for SmithKline Beecham and for Bayer. He has also held positions in R&D, regulatory affairs, process development, and manufacturing at other major pharmaceutical companies. He has successfully licensed products in the biologics, drugs, and device sectors on all six continents. Calcott holds a doctorate in microbial physiology and biochemistry from the University of Sussex in England. He has been a consultant for more than 20 years to government, industry, and academia.

ABOUT US

PHARMACEUTICAL ONLINE

Pharmaceutical Online's mission is to facilitate connections and foster collaborations in the small molecule drug development and manufacturing space. We deliver exclusive, actionable information to help industry professionals tackle the challenges they face in bringing high-quality therapies to market quickly and efficiently.

These insights, analysis, and best practices come from interviews with — and contributed articles from — recognized experts in the field. Topics covered include: Pharma 4.0 (AI, Big Data, automation, continuous manufacturing, etc.); regulations/cGMPs; facility design; process development; technology/equipment (filling, material handling, isolation, inspection, etc.); qualification, validation, and verification; quality management; supply chain; packaging/serialization; and logistics.

PharmaceuticalOnline.com
info@PharmaceuticalOnline.com
814.897.9000
5340 Fryling Rd., Ste 300, Erie, PA 16510