Bioanalysis ZONE

IDBS

The role of digital data management in today's collaborative drug discovery approach

fsg

Contents

Technology Digest: The role of digital data management in today’s collaborative drug discovery approach

by Olivia Seifert
Digital Editor, Bioanalysis Zone

Background

The initial stages of drug discovery and preclinical testing represent some of the most labor-intensive, and therefore costly, phases of drug development, with just 0.02% of the compounds entering preclinical testing progressing to clinical trials [1]. Consequently, ensuring that the processes mediating these stages are conducted meticulously is of utmost importance. For example, bioanalysis techniques generate critical data during discovery and development that are integral for early clinical programs [2]. A sensitive and specific bioanalytical technique is essential [2] along with diligent data management. This is no small feat; with evidence suggesting that there was an 11% increase in growth within the preclinical pipeline between 2021–2022 [3], creating the need to increase throughput, often with the same resource. Many drug candidates may be brought forward by biotech companies that lack the infrastructure to develop them [4]. To mitigate this issue, market trends within the biopharma industry towards outsourcing continue [4], as collaboration is increasingly recognized as vital in providing the speed and experience needed to effectively tackle the early discovery and preclinical stages of the drug development lifecycle [1,4].

The role of contract research organizations (CROs) and emerging digital technology

Alongside the growth of the concept of collaborative virtual biotech companies, the global CRO market has blossomed and is anticipated to reach USD$7.8 billion in value by 2027 [1]. CROs are relieving the growing pressure on biotech and biopharma companies to increase research and development capacity and consequently need to be efficient to increase their throughput. The CROs’ challenge is to deal with the increased demand for the same resources, in order to meet the sponsors’ requirements, whilst maintaining confidence in data quality to ensure patient safety later down the line. This is particularly important at the bioanalysis stage where the data has implications for clinical trials on patients. The market is competitive and building trusted relationships between CROs and their biotech/biopharma sponsors, to ensure partnership continuity, relies on expectations of robust data management, scientific expertise and efficiency in reaching milestones [6].

Digital software technologies have been developed to assist CROs and biotech companies with these issues. Many larger biotech companies have invested in a range of software that is typically brought together utilizing in-house integration code and analytical tools [4] or instead creates data silos. Data management often relies on sample-based informatics systems – such as laboratory information management systems, or LIMS – and miss the full view of data that is required to provide the experimental context for rapid reporting and the insight for decision-making.

Another problem biotech and biopharma companies face is that, as technological innovation and investment are often gradual, commitments to old software can often hinder investment into more efficient novel technologies [4]. Further, a large proportion of biotech companies simply do not have the technical or budgetary means to build a platform of hardware and software to meet their needs and still rely on manual processes [4]. As they seek to maintain competitiveness, CROs can address this challenge as spreading their investment in new software platforms to service the needs of multiple biotech clients is more cost-effective.

Nowadays, software technologies on the market offer an integrated solution to driving Industry 4.0 aims in the biotech space – accelerating operational efficiency, reducing costs and decreasing time to market [4]. When choosing whether to implement such technologies, CROs and biotech companies must consider several factors.

Technological considerations

One of the key concerns for CROs is quality assurance. Stringent regulatory requirements can create a significant manual burden, impacting study cycle times [7]. Consequently, investing in an integrated digital platform can provide real-time quality control to ensure that inventory, equipment and experimental results are within expected validated method limits and prevent deviations at the time of execution.

Maintaining data integrity also represents a significant issue; by the end of 2021, 65% of all '483s' warning letters issued by the FDA concerned data integrity violations [8]. Manual transcription utilizing human operators risks introducing errors into data, with each additional transcription required in the data transfer process increasing the chance of data integrity issues [4]. By introducing processes including barcode scanning, hands-free, voice-enabled data entry and system integrations, digitalization can ensure that data retain its integrity.

CROs should consider that integrated data management software platforms can aid CAPA – corrective action, preventive action – risk reduction. A connected digital view makes reporting for audits quick and efficient; information can be obtained directly from a single screen view, as opposed to requiring a paper chase through multiple physical records. It can also strengthen system security, as platforms can ensure cloud-based data is only accessible to specific project collaborators to provide secure areas for data transfer and collaboration.

In addition to addressing data integrity and security concerns, digitalizing processes can provide greater insight during the drug discovery cycle; capturing data in experimental context at the point of execution, alongside powerful analytic capabilities, supports data connection and comparison to enable reporting directly from a single view. Further, by reducing study cycle times through increasing operational efficiency and the ability to provide greater insights and confident recommendations [7], CROs can support sponsors to accelerate through milestones.

Overall, software investment that supports integrated workflow execution, real-time quality control and contextualized easy access to study data for rapid reporting has already been shown to accelerate client milestones by improving operational efficiency [9]. Further, technological investment can lay the foundations for trusted, ongoing collaboration between biotech companies and CROs, as it enables the highest standard of data integrity and business continuity – all data and methodology are traceable to create reproducibility within and across teams.

Investing in cloud-based technology platforms

Investing in integrated technology platforms to help outsource key processes within the drug development lifecycle can clearly offer a multitude of benefits to the biotech industry. Further, CROs able to drive effective bioanalytical workflows are expected to experience the highest rates of growth [1], making an investment into such platforms an attractive prospect. Indeed, Sheila Breidinger of Merck (NJ, USA) reported that "having experienced CROs that are equipped with the latest technologies to be able to support bioanalysis in the future is going to be critical." [10]

One platform, Polar BioAnalysis from IDBS, has been developed to provide CROs and BioPharma companies with the chance to improve the efficiency, quality and reproducibility of their bioanalytical studies, decrease study cycle times by up to 55% and accelerate market launch [11]. To achieve this, Polar BioAnalysis's integrated platform facilitates bioanalytical studies, from registration to the planning, execution and reporting stages. In addition, the platform mitigates the risk of data incompleteness, increases the degree of automation to reduce the risk of data entry and method deviation errors and allows full traceability in the workflow. Overall, it allows streamlining workflows, quality assurance and increases collaboration across teams to accelerate milestones.

Brought to the market by IDBS (Surrey, UK), Polar BioAnalysis has already successfully helped leading CROs and biotech companies with their bioanalytical workflows; one CRO customer reported a 20–30% increase in operational efficiencies, after investing in the IDBS platform to help improve method execution consistency and data quality and - enhance its ability to support sponsors to bring life-changing therapies to the market faster [9].

Sponsorship & disclaimer

This article has been drawn from discussions from a Technology Digest article published in Bioanalysis Zone, sponsored by IDBS. The opinions expressed in this feature are those of the author and do not necessarily reflect the views of Future Science Group.

Financial & competing interests disclosure

At the time of writing, O Seifert was an employee of Future Science Group. The author has no other relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript apart from those disclosed.

No writing assistance was utilized in the production of this manuscript.

References

1 Pharmaceutical Outsourcing. The Importance of Effective Data Capture and In-Lab Tech for Bioanalytical CROs: Implications for Quality and Customer Satisfaction (2020). [Accessed 29 September 2022] https://www.pharmoutsourcing.com/Featured-Articles/568514-The-Importance-of-Effective-Data-Capture-and-In-Lab-Tech-for-Bioanalytical-CROs-Implications-for-Quality-and-Customer-Satisfaction/

2 Pandey S, Pandey P, Tiwari G, Tiwari R. Bioanalysis in drug discovery and development. Pharm Methods. 1(1), 14-24. (2010) doi: 10.4103/2229-4708.72223.

3 Pharma Intelligence. Pharma R&D Annual Review 2022 Navigating the Landscapes. (2022) [Accessed 07 October 2022] https://pages.pharmaintelligence.informa.com/rdreview?utm_source=RDReview2022&utm_medium=whitepaper&utm_id=2296624620#

4 PharmTech. An Integrated Approach to the Data Lifecycle in BioPharma (2022). [Accessed 29 September 2022] https://www.pharmtech.com/view/an-integrated-approach-to-the-data-lifecycle-in-biopharma

5 Craddock A, Nadarajah S. Future trends in outsourcing: a summary of the Bioanalysis Zone survey. Bioanalysis 9(15), 1127–1129 (2017) doi: 10.4155/bio-2017-4985.

6 Redica Systems. Data Integrity Trends in 483s and Warning Letters: Part 1 (2019). [Accessed 29 September 2022] https://redica.com/pharma-medical-devices-data-integrity-breaking-down-keywords-and-citation-trends-from-the-fda/

7 PharmaIntelligence. What Does The Pharma Industry Want From CROs? (2022). [Accessed 29 September 2022] https://pharmaintelligence.informa.com/resources/product-content/what-does-pharma-want-from-cros

8 Regulatory Focus. Experts say FDA enforcement focus unchanged, use of alternative tools to grow (2022).
[Accessed 29 September 2022]
https://www.raps.org/news-and-articles/news-articles/2022/6/experts-say-fda-enforcement-focus-unchanged-use-of

9 IDBS. A Top Ten CRO Deploys IDBS Polar for Faster BioPharma Development (2022).
[Accessed 29 September 2022]
https://www.idbs.com/2022/01/top-ten-cro-deploys-idbs-polar-faster-biopharma-development/

10 Breidinger S, Chaudhary A and Woolf E. Current status of bioanalytical outsourcing: a pharma perspective. Bioanalysis 3(20), 1165–1169 (2017) doi: 10.4155/bio-2017-4990.

11 IDBS. Transforming Your Bioanalytical Operations (2022).
[Accessed 29 September 2022]
https://www.idbs.com/2021/05/transforming-your-bioanalytical-operations/

For reprint orders, please contact: reprints@future-science.com

Bioanalysis

Cloud solutions for GxP laboratories: considerations for data storage

Scott Davis*,[1], Joel Usansky[2], Shibani Mitra-Kaushik[3], John Kellie[4], Kimberly Honrine[5], Eric Woolf[6], Jeb Adams[7], Ryan Kelly[8], John Evens[9], Samuel Pine[10], Hannes Hochreiner[11], Michelle Dawes[12], Jason Kentner[13] & Sean Crawford[14]

[1]Information Technology, PPD, 2240 Dabney Road, Richmond, VA 23230, USA
[2]Research & Early Development, Bristol Myers Squibb, Princeton, NJ 08648, USA
[3]Bioanalytics-Genomic Medicine Unit, Sanofi, Framingham, MA 01701, USA
[4]Bioanalysis, Immunogenicity & Biomarkers, GSK, Collegeville, PA 19426, USA
[5]Automation Group, PPD, Richmond, VA 23230, USA
[6]PPDM – Regulated PK Bioanalytics, Merck & Co., West Point, PA 19486, USA
[7]R&D Operations, Amgen, Inc., Thousand Oaks, CA 91320, USA
[8]R&D – Software, Sotax Corporation, Westborough, MA 01581, USA
[9]Immunochemistry, PPD, Richmond, VA 23230, USA
[10]Bioanalysis & Immunogenicity, Nanobody Research Platform, Ablynx NV, a Sanofi Company, 9052 Zwijnaarde, Belgium
[11]R&D Informatics, Merck KGaA, 64293 Darmstadt, Germany
[12]Nonclinical Disposition & Bioanalysis/Nonclinical Research & Development, Bristol Myers Squibb, Princeton, NJ 08648, USA
[13]Information Technology, KCAS Bioanalytical & Biomarker Services, Shawnee, KS 66216, USA
[14]Commercial Data Science, Business Insights & Analytics, Bristol Myers Squibb, Princeton, NJ 08648, USA
*Author for correspondence: Tel.: +1 804 690 3581; scott.davis@ppd.com

Challenges for data storage during drug development have become increasingly complex as the pharmaceutical industry expands in an environment that requires on-demand availability of data and resources for users across the globe. While the efficiency and relative low cost of cloud services have become increasingly attractive, hesitancy toward the use of cloud services has decreased and there has been a significant shift toward real-world implementation. Within GxP laboratories, the considerations for cloud storage of data include data integrity and security, as well as access control and usage for users around the globe. In this review, challenges and considerations when using cloud storage options for the storage of laboratory-based GxP data are discussed and best practices are defined.

First draft submitted: 18 June 2021; Accepted for publication: 26 August 2021; Published online: 13 September 2021

Keywords: cloud storage • data integrity • validation

Challenges for data storage during drug development have become increasingly complex as additional laboratories are introduced across international and multisite companies. As the pharmaceutical industry expands in an environment that requires on-demand availability of data and resources for users across the globe, the efficiency and relative low cost of cloud services has become an increasingly attractive option. As hesitancy toward the usefulness of cloud services has decreased, it has become apparent that there has been a significant shift toward real-world implementation of such services. Within regulated environments such as GxP laboratories, there are many considerations when moving to the cloud in terms of data integrity and security, as well as more practical notions regarding how access is controlled and how data can be accessed by global users. In this white paper, we will discuss the challenges and considerations when using cloud storage options for the storage of data for lab-based GxP organizations, defined here as organizations that follow GLP, GMP and/or GCLP regulations.

Utilizing cloud providers

The information technology needs of the pharmaceutical industry are following trends apparent in other industries, necessitating a move toward cloud providers. However, there are limitations and concerns regarding regulated data being stored and transferred into a cloud-based environment. Pharmaceutical companies and industry partners

newlands press

providing sponsor- and study-related services are bound by health authority regulations regarding data integrity, security, privacy and other considerations that do not have many parallels in other industries. In the guidance document, *Data Integrity and Compliance with CGMP*, the US FDA acknowledges that sponsors may choose to outsource electronic services, including cloud computing. As such, the FDA notes that sponsors 'implement appropriate controls to manage risks associated with each element of the system' [1]. This not only implies the regulatory expectation that sponsors perform and document due diligence on any provider prior to engagement but also implies that an organization can use cloud storage for its data needs if desired. With these implications in mind, what are some considerations for the use of cloud storage?

There are various cloud offerings available that can suit the needs of just about anyone, from a single user at home to the largest worldwide organization. As always, any organization looking for a new provider wants to find the best service and value for the cost invested. However, it often can be confusing when one looks at what a provider offers and making 'apples-to-apples' comparisons can be difficult at the least, and positively painful at the worst. For example, if one browses to the 'Explore Our Products' page for one of the major cloud services provider, Amazon Web Services^{TM} (AWS) [2], there are over 20 categories of products to choose from and well over a hundred actual services. Similar lists of Microsoft Azure [3] and Google Cloud Services [4] offer up the same bountiful list of cloud-based service options. Factor in hundreds, if not thousands, of other smaller cloud service providers and the sheer number of options can boggle the mind. How does one go about traversing the universe of potential options that are available?

Cloud service provider requirements

The first step in any such endeavor is to determine an organization's actual cloud service needs. For example, is the need to simply identify options for data storage options or would statistical analysis of the web traffic or other metrics be needed? Is the scope determined to be a virtual data area that would serve 50–100 people or a far larger access pool? Can the organization afford to maintain and expand internal data storage, or can it benefit from the scalable, on-demand nature of the cloud? Does the organization need constant access to work with the data while in the cloud, or just long term, read-only storage of the data is needed? Before contacting any service providers, these definitions of 'need-to-have' and 'nice-to-have' requirements should be worked out with the data users and owners within each organization. It is very helpful to define what the needs really are and make a list of requirements that describe exactly what is needed from a potential provider, including storage requirements for the data.

The storage requirements for electronic records should meet GxP requirements, where applicable, and the protection of the data should be maintained throughout the life cycle of the retention period through a chain of custody process [5–8]. Data should be readily available at any time according to the defined needs, with the caveat that large datasets stored offsite or in the cloud may require additional lead time to download and restore. The original file format will need to be retained, which may require companies to maintain older versions of software, computers or databases to ensure the data can be accessed when it is needed [9]. For example, hard-copy printouts or nonhuman readable formats will not be acceptable during most health authority inspections [5].

Considerations for data storage

Once, the requirements for potential cloud providers have been determined, it is time to look at considerations for the targeted data. Information security and privacy is a major consideration when considering a cloud provider. The foundation of this is the 'CIA' triad of confidentiality, integrity and availability of data. The confidentiality of sensitive and critical data must be maintained. In order to prevent disclosure of proprietary information, data should be stored in a secure and preidentified/mapped space set aside for the organization and should not mingle with files from other clients of the vendor. Access must be controlled to ensure that no unauthorized user can access any files, the current data owners have stored in the cloud solution. Controls on access to the data also maintain its integrity. The vendor should provide evidence that files are not accessible for corruption over their lifetime on the cloud, which can extend into years or decades, and that data integrity is maintained. Confirmation tests that demonstrate that files do not change over time should be performed, either by the vendor or user's organization. There should also be audit trails, so that access to a file can be tracked as well as any changes from authorized users. Availability considerations are also important, as some data one may need to access constantly, while other files can stay in stasis in the cloud, untouched for years. Most cloud providers charge differently for file storage depending on the type of specific access controls and auditing services users require. As a result, consideration of the types of availability one needs for the data cloud storage could result in major cost savings in the long term.

In the end who is responsible for security in the cloud? Is it the customer, the service provider or a shared responsibility? The answer to this depends on the cloud-service model; and in this white paper, we focus on an Infrastructure as a Service model (IaaS) or cloud storage. Other available service models include Platform or Software as a Service, respectively. In an IaaS model, which includes Microsoft® Azure®, AWS and Google Compute Engine™, the service provider is only responsible for the security of the physical data centers and other hardware that power the infrastructure. This means that customers must secure their own data and operating systems. Some specific elements of cloud security to look at should be identity and access management (how is access controlled, integration with the data generator, owner or the user's organizational IAM system, multifactor authentication capabilities), physical security, encryption and next-generation firewalls. Regardless, a multilayer approach should be a must.

A study by McAfee® [10] in 2020 illustrates an increase in cyber attacks against cloud services. Most high-profile breaches were a result of user missteps or misconfigured services versus being the fault of the service provider. Working with cloud providers can be an unchartered territory for biotech companies. Any company considering adoption of cloud storage services needs to start with documenting where the service provider's security ends and where the data owner's company's security begins and is that sufficiently covers the security and integrity needs.

Third-party data standards

Third-party standards may be cited by cloud providers to potential clients as mitigation of compliance concerns. Adherence and certification to these standards are mentioned by providers as part of their effort to market themselves as suitable for regulated records. Examples are ISO standards [11], SOC [12] certification and Fedramp [13]. As different standards cover different types of compliance under different circumstances, it is best to evaluate the specific focus of the organization to determine which standards apply and then search for a provider that adheres to these standards. If a provider claims adherence to a certain standard, it is highly recommended to be sure to request evidence that backs up any claims of compliance. Some standards require recertification after a certain period of time, so it is best to ensure that any potential provider is up to date on any claimed certifications.

IaaS considerations

The previous discussion focuses on the direct use of cloud services by sponsors. Sponsors should also be aware of risks associated with indirect use of cloud services. For example, a contract research organization (CRO) that the sponsor employs may utilize cloud services as a component of its processes/infrastructure. Alternatively, a sponsor may contract with a vendor for use of an online software platform, which is in turn hosted on infrastructure of a third party. It is important to not only assess quality processes at the CRO or the validation of the online platform but also at the very least be aware of the relationships that may exist between these vendors and third-party providers with whom they contract.

In the instance of a vendor providing IaaS on a cloud infrastructure, it is important for the sponsor to ensure the vendor meets or exceeds many, if not all, of the same requirements as the cloud provider. Any employees from the vendor site involved in the IaaS platform should be trained in handling data in a cloud-based environment. Applicable employees could range from software developers to field service members and technical support involved in supporting the IaaS. All documentation and training certifications must be traceable and readily available to the sponsor.

Since the vendor has most likely already selected its preferred cloud provider for the IaaS, it becomes more important for the sponsor to evaluate the software vendor and its relationship with the cloud provider, rather than just the provider itself. Specific points of interest in evaluating the IaaS vendor include testing of deployments, vendor employee access to data and preservation of data. Sponsors should verify these items both meet regulatory and internal requirements. Vendors also should be able to supply reasoning behind their selection of the cloud provider. A Service Level Agreement (SLA) may be necessary with the third-party vendor.

One of the most important considerations when using IaaS in the cloud is GxP compliance. Typically, laboratory data workflows must handle data inputs from various equipment and software sources (e.g., immunoassay, multiplex or LC–MS/MS instruments and data analysis packages). However, formats that are specific to a single vendor may become an obstacle for optimal compliance with regulations. Potential use of vastly different data processing and vendor-specific software could lead to a disconnect between different laboratories within a company or if assays must be transferred to CROs. If large datasets can be generated that do not feed into a simplified laboratory information management system (LIMS), or if gaps or differences in data processing workflows exist, this creates risk for data management.

Progression of software versions over time may also pose an audit risk, especially if newer versions of software lead to different processed results. The software life cycle should, therefore, be an important consideration if datasets may be needed for long-term program support. If used to support filings, software version updates need to demonstrate result equivalence with backwards compatibility for compliance during audits. When data are exchanged between companies (e.g., CRO to sponsor, or during a company acquisition), the contract should include language that mandates that raw data, including the versions of the software used to generate the raw data, are provided to the recipient. This could avoid any last-minute and costly software transfers down the road. There also have been cases where the raw data and test results are transferred to the sponsor's site where the subject matter experts (SMEs) process them using internally developed software to generate the test results. Security of the data during the transfer presents risk, especially if there are manual transfer steps. Sponsors have used data transfer via the cloud at a time when the procedures for validation cloud-based systems are not clear among the users and regulations are still not available.

It is also critical that software retains full backwards compatibility to older versions of file formats and data analysis algorithms. There are two issues to consider:

- The format of the data file changes over time (e.g., analogous to the switch of Microsoft Excel® from .xls to .xlsx) and newer versions of the software cannot open older versions of data files (i.e., a lack of backwards compatibility).
- The analytical algorithms used may have changed over time in the software due to bug fixes and/or improvements in analysis algorithms. If the latest version of the software only contains the latest (i.e., 'best') algorithm, then analysis of old data will yield different results.

These types of problems represent a severe risk to the company because upon an audit, the inspector may, for example, say, 'please show me the chromatogram and result values for sample X.' If the old raw data file cannot be opened, or if the algorithm has changed and the new software yields different numerical values, then the individual will be unable to demonstrate how the results reported to the auditor were obtained. This illustrates noncompliance with GLP and other GxP regulations. The solution to these problems is to apply pressure on software vendors to ensure full backwards compatibility to all versions of data files from their software and that all historical data calculation algorithms are available in the latest versions of their software. However, as this may not be realistic, each organization should be responsible for keeping older versions of software in case one needs them to recreate raw data results. Another consideration is to work with instrument and software vendors to adopt a secure, vendor-neutral data transfer process to avoid differences in file type and to allow secure, compliant transfer of data from system to system, or from data owner's organization to the cloud. It is envisioned that in the future, such a process will become more attractive and will be demanded by various organizations in the pharma space, and as such, initiatives of this type are already in process [14].

Sponsors also should focus on review of the Quality Management System of the provider and its alignment with regulatory expectations and company-specific requirements. Quite often, the sponsor has more expertise with regulatory expectation and should use the due diligence process as an opportunity to educate the supplier. Beyond the Quality Management System, other areas of focus include determining the geographic locations of provider facilities with emphasis on identifying whether it is possible for the end user to restrict data to defined regions. Training practices and awareness of staff regarding regulated data should be examined. The supplier should maintain explicit documentation of who within the providers organization has access to control the infrastructure. Organization charts, role definitions and job descriptions should be available for review. Finally, one should confirm the supplier maintains robust change control procedures for infrastructure and process.

External audits

An important topic to discuss with a potential vendor is how open the vendor is to external audits of their functions. For example, an organization may want to do a technical review of how it handles security, or even a compliance review to see how it meets any applicable regulations. This should include the rights for vulnerability and penetration testing and patch management compliance. Depending on the vendor, one may find some are very open to any audits requested, while others are not. It will be up to the storage service users (i.e., the potential customer), to determine how comfortable one is with a vendor's openness to outside audits. Beyond the data owners' organization's internal audits, the prospect of a regulatory audit also should always be discussed. The legal right of regulatory authorities to inspect cloud provider facilities is a topic of debate centered around whether the cloud provider facility is viewed as a 'test facility,' 'CRO' or other entity. Suppliers should know or be informed that they could become an inspection target for regulators, and that they should have procedures for handling this eventuality. All items mentioned previously, including the sponsor's documentation associated with provider due diligence, SLAs and customer agreements should be readily accessible to sponsor personnel who may be called upon during regulatory inspections at the sponsor site.

Selecting a vendor

Once, the cloud storage users have the requirements prepared, it is time to determine what vendors should be solicited for proposals for service scope and cost determination. It is recommended that new and existing users are using their requirements as a guide. For example: Does the current organization or user need the huge resources of Google Compute Engine™ or AWS, or perhaps something on a smaller scale? Next, the users should work out a short list of potential vendors and contact them. Include both large and small providers in order to get exposure to what services each type can offer. To initiate the dialogue, one must provide the requirements and work with the cloud service providers to determine what sort of options are available for next steps of the service request. It is highly recommended that users remember that this is the time for the vendors to impress and suggest a wide set of options. As a service seeker, the users should ask questions, ensure that the vendor clarifies everything being provided and risks versus benefit of every item on the list of services in question. If a vendor is not responsive to the users' needs that is the first sign that they are not a promising and dependable long-term service provider for these needs.

After all the above-mentioned steps, a list of acceptable vendors and potential cost information for each should become available. The last thing to consider is if one can obtain feedback from any present customers with each vendor to discuss their service experience. Vendors may often be willing to give out a customer contact, or data owners may already know someone who is using similar cloud storage services. Data owners are strongly cautioned to not ignore this potential source of vendor information, because it may help solidify the final choice of vendor decision. Once the decision makers have everything, one should have enough information to choose the vendor who is best suited to the needs and wants of the project and the progression to final decision on vendor selection may be made with well-informed data and confidence.

Service level agreement

When the step of vendor selection is complete, a SLA should be put in place between the sponsor and service provider. This document clearly defines the services, the provider will deliver along with associated timelines, including responsibilities of all involved parties. Examples of activities that might be included in the SLA are system backup and restore, downtime and restoration of service timelines, geographic restrictions on location of information and options regarding disposition of data on termination of agreement or in the event of lack of payment. Other considerations for the SLA are the description of records, materials to be archived, materials to be transported (i.e., physically or electronically), chain of custody, responsible individuals with access, storage requirements and conditions, the method for retrieval and access, and quality activities performed [6,7]. Another important consideration for a GxP laboratory is how the local regulatory authority views cloud-based services. Although OECD/GLP has not codified this in a written guideline, in recent years some GLP inspectors working under OECD guidelines have found fault in the use of a cloud-based service for providing data storage for GLP labs, for example. The most common finding is that the data are not always under the control of the testing facility. Although the topic is under discussion in many regulatory bodies, the sponsor is ultimately responsible for their own data and should evaluate any cloud-based providers' experience and ability to address regulatory findings, especially in the GLP space.

Part of a risk-based vendor management plan should include contingency plans if any vendor is no longer able to provide a service. This is also true for cloud-based data storage providers. If the external vendor goes out of business or has no legal successor, it should be specified that the materials and records should be transferred back to the sponsor in a validated and tested manner [6,7]. Sponsors should demand transparency from the ground up and maintain clear data paths that are traceable and compliant with regulator and sponsor requirements and expectations. Large service providers, such as AWS, typically have standard agreements already developed that the vendor may be reluctant to modify. In such cases, an additional document, sometimes called a customer agreement, may serve to supplement the standard SLA. In addition, relevant standard operating procedures (SOPs) should be created, enforced and followed by both parties. The SOPs should define how and when data will be accessed and what approval is required.

Migrating data to the cloud

It is important that all data required for reconstruction of the study be migrated, including metadata, audit trails, e-signatures and associated hardware and software [8]. When migrating electronic records, this process should be fully documented and validated to ensure it is complete and accurate. The conversion of data to a different format (i.e., from a proprietary data format to common format, such as PDF) should be considered as data migration. Where data are transferred to another medium, data must be verified as an exact copy prior to any destruction of the original data. Files considered archived should also be in a read-only status. The value and/or meaning and links between a system audit trail and electronic signatures should be ensured during the migration process. There may be a need to produce duplicates of the electronic records to ensure preservation; however, the duplicates will be individually maintained, verified and tracked [1].

Continuing relations with the service provider

Once everything is in place and users and owners are using a new cloud service vendor, it is recommended that they keep in regular contact with the support team to ensure any questions are answered and issues remediated. This also will allow the vendor to update cloud users on any new services or rate changes. As always, a vendor will want to place the latest and newest service, but it is very important that if the service users consider any new services offered with short- and long-term insights into how the new or upgraded version will enhance existing business needs and balance the benefit with the cost impact. While new services often can be very helpful, newer does not always mean better, especially in the GxP space, so it is expected that the vendor fully justify any new service offered before upgrading or changing anything in the system.

Case study

The following case study demonstrates the potential gaps between a full or hybrid cloud solution for data management and storage.

Data capture

Immunoassay (ELISA) data are captured on a plate reader (e.g., Molecular Devices SpectraMax® Plus 384), and read using proprietary software (i.e., SoftMax® Pro). Both metadata and raw data are generated during the read, and all are stored in the proprietary data file. In the case of GxP work, the audit trail for these data is also contained in the file. The audit trail contains multiple elements:

- A log of all actions taken by users, date/time stamped, with user name attributed;
- Plate reader information, software version and the location where the data file has been saved;
- Read specifications – such as type of measurement (e.g., absorbance), wavelength and auto-mix settings.

It should be noted that the number of steps in data processing and their complexity can vary widely from instrument to instrument, and the retention of intermediate data also will vary.

Data format

The raw data file that is produced is in a proprietary data format (.eda or .sdax [versions 6.0 and higher]). Often, the raw data must be exported and converted into a .txt file for import into a LIMS application. This means that both the binary data file (containing further metadata and audit trail) as well as the exported plain-text file must be retained and traceable.

Data transfer

Data transfers are handled in several steps, both automated and manual. First, the proprietary data file is manually saved to a network location using the ‘Save As’ command, such as a folder related to a particular study. The user then exports the data as a .txt file to the same location and prints the data to a PDF file, also saved in this location.

After approximately 15 min, the data are swept to a read-only location on the network to ensure that the files can no longer be edited. The 15-min timeframe gives the analyst time to generate and save the data files, but not too much time to allow for any further changes. The data files will reside in the read-only project directory until the end of the project. At that time, the data are swept to a cloud location for archive storage. The location on the third-party cloud is specific to the organization performing the assay and is not mixed with other clients of the cloud provider. At this point, the files are read-only and fall under the purview of the archivists of the organization.

Data restore

If data files need to be restored to the network, users must contact the archivist, who then can restore the files to an appropriate network location from the cloud. Alternatively, users can also be given the option to browse the cloud location themselves and restore copies of any files needed but must contact the archivist to have any new copy put into archives with appropriate approval. The audit trail and version history of the file will be kept in the cloud, if needed. For the purposes of most audits/retrieval efforts, the PDF of the raw data serves to make the raw data easily viewable from any computer without the need for the Softmax Pro software. If the audit trail needs to be reviewed, this can be accomplished by either opening the raw data file through the Softmax Pro software or through a text editor. It is important to note, however, that the original (complete) data values and a good portion of the metadata are only viewable through the Softmax Pro software [15].

Commentary

As instruments have grown in their sophistication, so has the nature of the data captured. Often, there is a heavy reliance on file-naming conventions and nomenclature to determine, which file was derived from another. Additionally, to review the data flow process, multiple files (which often are copies in different formats) must be viewed and each tracked. The number of files for data types has increased (e.g., images), as well as their size. The exact nature of what raw data is captured and the size requirements, as well as the complexity of traceability should be considered both when implementing a new instrument as well as when choosing data storage infrastructure.

Additionally, since there are multiple software packages used in the process, there are differences with how data are grouped and organized in each. For example, software to sweep from instrument computers to a network location, as well as off-the-shelf archiving solutions, are often scoped per instrument. This means that if multiple instruments are used to generate data for a single study, their data will be in separate folders in both the network drive and archiving tool. This necessitates the manual compilation of data into study or project-specific folders. This can also lead to multiple copies of data in various locations, all of which may need to be explained and traced during an audit.

Conclusion

The data generated in a process or workflow can be the most important aspect of a business. Handing this precious resource over to a third-party cloud service often can add functionality, security and safety to the data but it also can be daunting to evaluate and select from the incredible number of vendors and services available, and then manage the vendor and data for its planned life cycle. It falls to the data generator or user – the potential cloud service customer – to fully evaluate any potential vendor and to keep tabs on any vendor contracted with the responsibility for the storage and management services. There are a multitude of responsibilities involved with keeping track of the support provided by the cloud service vendors. However, once a system is put in place, most end users will discover that cloud services greatly increase the efficiency and dependability of business development and continuity.

Future perspective

As the biopharmaceutical industry moves forward and cloud data storage becomes ubiquitous, it is expected that international regulatory authorities will reach consensus on how to handle working with cloud storage providers. Regional and local health authorities and laboratory regulators should, in turn, provide clarity on whether cloud service providers are eligible for audit as well as give a better understanding of organization roles and responsibilities. Also, guidance could be released on the appropriate security configurations for cloud providers in order to help organizations achieve better protection against the ever-expanding threat of cyber attacks.

Box 1. Definitions.

Cloud services: Computing services that demonstrate the characteristics of on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

Infrastructure as a Service (IaaS): The first of three models of cloud services providing processing, storage, networks and other fundamental computing resources upon which the customer is able to deploy and run arbitrary software, including operating systems and applications.

Platform as a Service (PaaS): The second model of cloud services, providing all the resources of IaaS, plus operating systems. The customer is able to deploy applications on the platform and may have some control over configuration of the application hosting environment.

Software as a Service (SaaS): The third model of cloud services where a software application runs on a platform and infrastructure controlled by the provider. The application is accessible to the customer through a browser or program interface.

Confidentiality: Only authorized users and processes should be able to access or modify data.

Integrity: Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously.

Availability: Authorized users should be able to access data whenever needed.

Service Level Agreement (SLA): Defines the level of service expected from a vendor, laying out the metrics by which service is measured and the remedies or penalties if not met.

Executive summary

With regulatory compliance and cyber security risk associated to the 'CIA' of data, understanding the caveats and ramifications of cloud solutions can help laboratories determine the feasibility of moving resources to that type of services.

Background

- Complex options available related to cloud solutions including various cost structures.
- Hesitancy has decreased over time, and a shift toward cloud services.
- Many considerations are required for GxP organizations in consideration of a move.

Discussion

- Determination of where to use cloud services.
- Data retention periods, short-term, long-term needs.
- GxP requirements of a cloud solution.
- Type of cloud services.
- Securing cloud services – who has the responsibility.
- Third party standards and certifications.
- Service Level Agreement considerations.
- How to select a vendor.
- Auditing considerations.
- Data migration options.

Conclusion

Data are the most important aspect of the GxP organization. Storage complexity and requirements are increasing, and cloud solutions can be an attractive option for maintaining this ever-growing pool of data. Where considerations are addressed, organizations can find ways to safely and effectively embrace these cloud solutions to increase efficiency with which data users and owners do their business.

Financial & competing interests disclosure

The authors have no relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript. This includes employment, consultancies, honoraria, stock ownership or options, expert testimony, grants or patents received or pending, or royalties.

No writing assistance was utilized in the production of this manuscript.

References

1. US FDA. Data integrity and compliance with CGMP Guidance for industry (2016). https://www.fda.gov/files/drugs/published/Data-Integrity-and-Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf
2. Amazon Web Services. Cloud Products. https://aws.amazon.com/products/?hp=tile&so-exp=below

3. Microsoft Azure. Products. https://azure.microsoft.com/en-us/services/

4. Google Cloud Platform. Products and services. https://cloud.google.com/products/

5. US FDA. 21 CFR Part 11. Electronic records; electronic signatures – scope and application (2003). https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

6. Working Group on Information Technology (AGIT). Good laboratory practice (GLP) (2016). https://www.anmeldestelle.admin.ch/dam/chem/de/dokumente/download-listen/aagit/agit-guidelines-external-it-service-providers.pdf.download.pdf/AGIT_Guidelines_External_IT_Service_Providers_EN.pdf

7. European Commission. EudraLex: the rules governing medicinal products in the European Union. Volume 4. Good Manufacturing Practice (2011). https://ec.europa.eu/health/sites/default/files/files/eudralex/vol-4/2017_11_22_guidelines_gmp_for_atmps.pdf

8. US FDA. Guidance for industry. computerized systems used in clinical investigations (2007). https://www.fda.gov/regulatory-information/search-fda-guidance-documents/computerized-systems-used-clinical-investigations

9. OECD. OECD Series on principles of good laboratory practice and compliance monitoring. Number 17. Application of GLP principles to computerised systems. Section 114 (2016). https://www.oecd.org/chemicalsafety/testing/oecdseriesonprinciplesofgoodlaboratorypracticeglpandcompliancemonitoring.htm

10. McAfee. Cloud adoption and risk report: work from home edition. https://www.mcafee.com/enterprise/en-us/forms/gated-form.html?docID=3804edf6-fe75-427e-a4fd-4eee7d189265

11. International Organization for Standardization. Standards. https://www.iso.org/standards.html

12. American Institute of Certified Public Accountants, System and Organization Controls. SOC suite of services. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html#:∼:text=System%20and%20Organization%20Controls%20(SOC,level%20controls%20of%20other%20organizations

13. FedRamp. Cloud service providers. https://www.fedramp.gov/cloud-service-providers

14. Arfvidsson C, Van Bedaf D, Globig S *et al.* Improving data integrity in regulated bioanalysis: proposal for a generic data transfer process for LC-MS from the European Bioanalysis Forum. *Bioanalysis* 12(14), 1033–1038 (2020).

15. Molecular Devices. SoftMax Pro data acquisition and analysis software version 7.0.2 User Guide 5049092B (2017). https://www.moleculardevices.com/sites/default/files/en/assets/user-guide/br/softmax-pro-data-acquisition-and-analysis-software.pdf

For reprint orders, please contact: reprints@future-science.com

Bioanalysis

Data integrity in regulated bioanalysis: a summary from the European Bioanalysis Forum Workshop in collaboration with the MHRA

Cecilia Arfvidsson[1], David Van Bedaf[2], Mira Doig[3], Susanne Globig[4], Magnus Knutsson[5], Mark Lewis[6], Stuart McDougall[7], Marco Michi[8], Nathalie Mokrzycki[9] & Philip Timmerman*,[10]

[1] AstraZeneca R&D, Gothenburg, Sweden
[2] Janssen R&D, Beerse, Belgium
[3] ABS Laboratories, Welwyn Garden City, UK
[4] Idorsia Pharmaceuticals Ltd, Allschwil, Switzerland
[5] Ferring, Copenhagen, Denmark
[6] GlaxoSmithKline R&D, Ware, UK
[7] ARCinova, Alnwick, UK
[8] Aptuit an Evotec Company, Verona, Italy
[9] MSD, Clermont-Ferrand, France
[10] European Bioanalysis Forum vzw (EBF), Havenlaan 86c b204, 1000 Brussel, Belgium
*Author for correspondence: chair@e-b-f.eu

In this conference report, we summarize the main findings and messages from a workshop on 'Data Integrity'. The workshop was held at the 11th European Bioanalysis Forum Open (EBF) Symposium in Barcelona (21–23 November 2018), in collaboration with the Medicines and Health products Regulatory Agency to provide insight and understanding of regulatory data integrity expectations. The workshop highlighted the importance of engaging with software developers to address the gap between industry's data integrity needs and current system software capabilities. Delegates were also made aware of the importance of implementing additional procedural controls to mitigate the risk associated with using systems that do not fully meet data integrity requirements.

First draft submitted: 30 May 2019; Accepted for publication: 5 June 2019; Published online: 27 August 2019

Keywords: audit trail • data integrity • data transfers • EBF

The aim of this workshop was to increase the insight and understanding of regulatory expectations in relation to the new Medicines and Health products Regulatory Agency (MHRA) Guidance on GxP data integrity, issued in March 2018 [1]. The workshop also aimed to provide further insight and guidance on how to implement adequate levels of data integrity control dependent on the criticality of the data generated. The workshop was built with input and support from EBF expert members, who shared some of their recent MHRA inspection findings, and in collaboration with two MHRA inspectors. Finally, the workshop gave the participants, representing various parts of the bioanalytical community, an opportunity to discuss and define the current gap between the regulatory data integrity expectations and the availability of compliant software; highlighting the need for re-focus and commitment from the software developers to support users to attain the goal of having systems that meet the industry's data integrity requirements and the Regulator's expectations, based on relevant guidance and legislation.

The Data Integrity Workshop

The workshop was introduced by the organizing committee, on behalf of the EBF [2], to give a brief overview of the data integrity concepts and the overall intention and content of the workshop. This was followed by a presentation by one of the participating senior GCP and GLP inspectors from the MHRA, on their view on how to implement

newlands press

the data integrity guidance. The presentation highlighted the importance of understanding the terminology in the guidance as well as the basic concepts. The MHRA recognizes the technical, organizational and cultural challenges of implementing data integrity governance, and that there are no quick fixes. Implementation should be considered to be a multi-disciplinary activity and extensive changes may be required which will have resource and financial implications. It was accepted that change of this scale and potential complexity will require time to complete, but implementation of controls should be prioritized based on a data integrity risk assessment. The MHRA elaborated further on two main data integrity concepts:

- Data lifecycle; that includes data collection, processing, reporting, review and archiving;
- Data governance; that includes the process, the systems used and the ownership of these systems.

When defining these concepts, you should examine the role and access rights of all individuals, review all internal and external data transfers and examine whether there are any stages where data can be altered or deleted. Once these are defined and examined then the next steps are to decide what is critical data as all data are not equal. An example was provided; 'The acceptance criteria for calibration standards and quality controls (QCs)'. Should a user examine what software was used to produce this data? Who looks at the data? What are the potential risks in generating this data and can the data be manipulated or inadvertently changed? In addition, can a QC or calibration standard ever be reinjected and the data replaced?

The full slide set from the MHRA presentation can be found on the 11th EBF Open Symposium web page [3].

The workshop progressed to discuss and provide feedback on two main data integrity themes – Data Transfer/Control and Audit Trails. The organizing team introduced a number of questions on each theme to promote interactive discussions, which are summarized below:

Theme 1 – Data transfer/control:

- How can we transfer data and ensure no modifications and/or deletions occur in the process?
- What documentation can we store with our study file to ensure that data integrity is maintained at each data transfer step?

Theme 2 – Audit trail:

- How are audit trails used to ensure modifications and/or deletions of data are identified and captured in line with data integrity expectations?
  - Why do we review the audit trail, what are the risks that we would like to mitigate?
  - How do we document the outcome of the review?
  - Should the audit trail review procedure be detailed in a standard operating procedure (SOP)?

In order to create an open and transparent atmosphere at the workshop and to set the scene for the round table discussions and panel, the above two themes were the primary focus in two case studies presented by two EBF member companies on recent MHRA inspection findings at their UK laboratory facilities.

In the first presentation, a summary of all the major findings was shared. This summary highlighted the challenge to the facility to ensure integrity and accuracy in the dataset when data acquired using for example the MassLynx™ (MA, USA) software was transferred into Watson™ LIMS (Thermo Fisher™, MA, USA). In this case, the transfer process included the production of a text file that, if not protected from modifications, could be edited and then opened in the LIMS system with an amended dataset. In isolation, the quality assurance review of the data, in the format it resides in Watson LIMS (Thermo Fisher, MA, USA) and with flat file representation of the chromatograms printed to the NuGenesis™ (MA, USA) system, could not be considered to be representative of the raw data.

In a second presentation, similar data integrity deficiencies with laboratory analyzers between their LIMS system and MS software were presented as a finding from another recent MHRA inspection. This presentation also highlighted the MHRA's acceptance of their step-wise remediation plan, which included a substantial length of time to implement the changes to obtain the necessary data integrity controls. The slide sets from the two case study presentations can be found on the 11th EBF Open Symposium web page [3].

Following the introductory presentations and the two case studies, the workshop continued with interactive round table discussions where the approximately 100 workshop participants had the opportunity to discuss their specific data integrity issues in smaller groups. The main questions and concerns from these discussions as well as from the room in general were then addressed in a concluding panel discussion (comprising MHRA representatives, Laboratory Managers and Quality Assurance [QA] professionals), summarized under each theme below.

Data transfer

In the introduction given by the MHRA on implementation of data integrity controls, a process map exercise was suggested as a valuable tool to visualize and to define your 'data flow and process' universe. The process map(s) should help to define the systems, processes, equipment and roles impacted and to identify the key interfaces and communication lines. The process map(s) can also be used to evaluate the time, process and data criticality of each step. In the following panel discussion, the MHRA clarified that the process map(s) should be a tool for the business to visualize their business processes and that they should not be put in place 'just to please the regulators'. By understanding the use of the data in each step of the map, it is possible to identify the critical data as well as the controls and oversight measures required for adequate risk mitigation. The MHRA presentation also highlighted how data criticality should be determined by the intended use of the data, and that there is an expectation that risk management principles will be used to assess the risks and to identify the necessary mitigation steps. The Panel were asked if a 100% QC check would ever be necessary for a manual/compromised data transfer step? In line with the previously conveyed risk management principles, the MHRA emphasized that the extent of any QC check would be dependent on the risks associated with the data generated. The importance of monitoring and documenting the outcome of any QC checking was also highlighted in order to verify if the applied QC process and its frequency was required and suitable.

During the round table discussions, the current lack of data integrity suitable software and interfaces was raised as a great concern. It was proposed that, as they become available, new software features should facilitate the data transfer process and possibly even standardize the integration functionality. The software vendor representatives who attended the workshop were not too optimistic about a full standardization; however, they did flag that there may be some 'low hanging fruit' that could be identified and/or implemented with improved software awareness and knowledge. One software feature suggested was to include a functionality that locked the path for the exported text files and then tracked the export event in the audit trail. Such a feature could allow for easy setup of a proper network area with no deletion permissions to significantly improve the data integrity. It is essential that as a community we push for enhanced data integrity control functionality.

As the discussions progressed the value of enhanced interaction and dialogue between the bioanalytical community and the software experts were also emphasized. Data integrity is now a primary focus for a bioanalytical laboratory when choosing new platforms/software and compliance must therefore also be considered by the software manufacturers when developing new software features. During the panel discussion, the MHRA reflected on this topic and pointed out the importance of knowing your software and having an awareness of what data integrity features are available; however, they recognized that not all instrument users were also experts on the software functionality. When purchasing new instrumentation data integrity features should be part of the evaluation. It was suggested that the vendor's knowledge of the system should be utilized to better understand the functionality available, for example, the terminology and interdependencies used within the security and permission modules and audit trails.

Audit trail

In the introduction by the MHRA they briefly touched upon audit trails and their expectation that everyone should know what audit trails were available on their system(s) as well as what they covered. Organizations should also know what audit trails are recording or not recording. A few questions were raised to gain the workshop participants' attention:

- Do you understand the terminology used in the audit trail?
- Who reviews audit trails and how regularly are they reviewed?
- Are these procedures documented in an SOP?
- Do QA understand what they are auditing?
- Can QA access and review data?

The MHRA highlighted the importance of understanding what 'normal' looks like in your audit trail in order to be able to identify any 'abnormal' activities within a reasonable timeframe and work effort. Finally, they shared some areas that are ‘red flags’ to inspectors. These were items such as full audit trails not being activated, standalone systems, manual data recording, manual data transfers and shared logins.

The MHRA data integrity expectation is, however, not a forensic approach, reviews will normally be targeted and driven by requirements covered in data integrity policies or SOPs. This was considered important because if the audit trail is only reviewed as part of the final QA, review problems will only be highlighted once the study has been completed.

The MHRA recognized the difficulties in preventing intentional fraud. To mitigate the risk of fraud, risk assessments should be made to identify weak points in a process and suitable measures put in place to make fraud more difficult to perpetrate and easier to detect. There is an acceptance that it is impossible to eliminate the risk of fraud and that residual risks will remain, but steps should be taken to minimize this risk.

Conclusion & future perspective

The key take home messages from the workshop can be summarized as follows:

- Know your software system data and processes;
- Map your processes to identify the potential risks and weaknesses;
- Reduce the risk by implementing solutions that have been identified as a result of improved software awareness and knowledge;
- Open up the dialogue for enhanced interaction between system vendors, pharma/CROs and regulatory authorities to understand current, and define future, system data integrity capabilities.

The workshop was very well attended with approximately 100 participants, representing various roles (laboratory operators and management, quality, IT) from both Pharma and CRO companies. The broad audience, together with the open and energetic atmosphere at the workshop, highlights the great interest and engagement in this topic. The EBF e-environment team will therefore continue to drive the topic and arrange additional opportunities for dialogue on this topic, such as new interactive workshops. The EBF may investigate how we can extend the interaction to the broader instrument/software manufacturers to facilitate an improvement in the interface solutions. Also, potential synergistic activities with the EBF new technology and automation teams may be explored. From the workshop at the 11th Open Symposium, there is a clear desire to discuss how different companies have implemented their process mapping and risk analysis, and what has been learned during the planning, implementation and follow-up; EBF intends to create a platform for these experiences and learnings to be shared among the bioanalytical community and we would welcome contributions to this theme at the 12th EBF Open Symposium in Barcelona (20–22 November 2019).

Acknowledgments

The organizing committee would like to send a special thanks to all the presenters and panel members during the workshop – J Wakelin-Smith and A Gray (MHRA), S McDougall (ARCinova), M Lewis (GlaxoSmithKline) and D V Bedaf (Janssen R&D). Thanks also to all the workshop participants for their contribution to an interactive and productive workshop.

Disclaimer

The views and conclusions presented in this paper are those of the European Bioanalysis Forum and do not necessarily reflect the representative affiliation or company’s position on the subject.

Financial & competing interests disclosure

The authors have no relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript. This includes employment, consultancies, honoraria, stock ownership or options, expert testimony, grants or patents received or pending, or royalties.

No writing assistance was utilized in the production of this manuscript.

References

1. Medicines & healthcare products regulatory agency (MHRA) – ‘GXP’ data integrity guidance and definitions (2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf
2. European Bioanalysis Forum (EBF). http://www.e-b-f.eu
3. 11th EBF Open Symposium slide decks: http://www.e-b-f.eu/bcn2018-slides/

Bioanalysis ZONE

Contact us

Editorial department

editor@bioanalysis-zone.com

Business Development and Support

advertising@future-science-group.com

This supplement is brought to you by Bioanalysis Zone in association with:

IDBS