Building a Smart Laboratory 2016

An introduction to the integrated lab

From the publishers of
scientific computing world
www.scientific-computing.com/BASL2016

Data integrity takes centre stage

The smart laboratory can help maintain data integrity. But, as Isabel Muñoz-Willery and Roberto Castelnovo of the consultancy NL42 discuss, the place to start is with an organisation's business needs, not the technology and informatics tools themselves

As Peter Boogaard highlighted in the most recent edition of *Scientific Computing World's Laboratory Informatics Guide*, 'data integrity' is the key concept in the laboratory. The regulatory authorities' concerns over the integrity of laboratory data have finally set a deadline for the pharmaceutical companies to be completely compliant. The paperless, smart laboratory is no longer an abstract fantasy, but is urgently needed as the best way to conform with these regulatory requirements.

Data integrity covers the whole product life-cycle and a variety of organisations have put together educational and training activities across Europe to address this issue. The US Food and Drug Administration (FDA) is in the lead for many opportunities to attend training remotely. The FDA's Office of Manufacturing and Product Quality (OMPQ) recognises the effort invested in training inspectors to detect signs of data management problems, and of altered or manipulated records. It has already shown readiness on informatics technologies and raised the bar in the understanding of data integration capabilities available today.

Pay attention to the design, not the tools

Regulatory authorities are finding more issues with data integrity than ever before. It is important to reduce the risk that the integrity of laboratory data might be compromised, by ensuring that controls are correctly implemented and appropriately managed throughout the entire life of a record. Ensuring strong data integrity requires attention to the design, operation, and monitoring of processes and systems involved.

Once again, we´re glad to contribute to this year's edition of *Building a Smart Laboratory* drawing on our knowledge of dynamics of laboratory informatics in Europe – and more specifically in South Europe. While our article in BASL 2015 more concretely described the dynamics of the Spanish economy, the different pharmaceutical companies' categories, and the relevance of cultural differences for international providers, this time we´d like to highlight the opportunities to implement a transformational change, revisiting existing processes, finding potential gaps in data integrity and introducing a higher level of automation.

"Many companies are now emerging with new, cloud-based products"

Let´s start by defining the processes required to ensure the integrity of the data. Data integrity is the assurance that data records are accurate, complete, and intact. Ensuring data integrity means protecting

original data from accidental or intentional modification, falsification, or even deletion, which is the key to reliable and trustworthy records that will withstand scrutiny during regulatory inspections. Company policies on data governance and the implementation of 21CFR/11 capabilities, available in most informatics tools, should be more than enough to ensure intactness of the data records. However many FDA warning letters are notifications of a lack of implementation of the rules and tools.

Informatics tools can help

Enabling the 21CFR / 11 capabilities that laboratory informatics tools offer today can potentially solve most of these issues. Even so, those capabilities need to be assessed during the selection process in order to ensure that they can be effectively activated in every key process, phase, and step. The impact of the misuse of these capabilities is of paramount importance: control of data integrity in terms of its accuracy disappears, as does protection against editing, modification, or deletion. All potential traceability of 'who, when, for what and why' for the record disappears.

There have been instances of people who were supposedly absent accessing the system, thus indicating that they had shared their username and password. There are multiple ways to resolve the users' competences while interfacing with informatics systems, through review of processes, procedures, and systems.

Data integrity is not only about accuracy and protection; the data should also remain within its original context and include its relationship to other data records. Ensuring the integrity of critical data and metadata is necessary for all computerised laboratory systems. Raw data, electronic records, and metadata depend upon their context within laboratory processes. Data integration is basically mandatory and requires that companies gain a good understanding of the necessary solutions and technical tools used to evaluate the potential level of customisation that providers claim for.

During one laboratory informatics selection process, we prepared an exhaustive request for information document, sent to more than 30 companies, receiving responses from about 20 of them.

Despite the fact that a very limited number have local representation in South Europe, many companies are now emerging with new, cloud-based products. Some have already developed specific relationships with key players in pharmaceutical companies, such as leaders in CRM, document management, and chromatography solutions. Yet the technical solutions provided for the interactions are far from being new and revolutionary. Some companies have the capabilities to develop drivers to interact with a long list of instrumentation; others rely on customisation, coding hours from their technical experts. One of the key issues in protecting data integrity is related to data integration. In most laboratory data management projects, it is important that the newly implemented systems are capable of interfacing with other existing systems (ERP, MES, EBR, DMS, QMS, CDS, etc.). Developing a solid and reliable integration is key to ensuring a successful audit on IT systems. There are obviously a variety of options on how data should be interchanged between systems, starting from a purely manual interface (data manually copied from one system to another) to a fully automated interface (no human interactions). First of all, it is critical that the most reliable and accurate process behind the integration is designed into the project. Secondly, it is critical to evaluate the risks associated with each technical option, develop proper procedures when a manual or semi-automatic integration is designed, and finally solid documentation should support the solution implemented.

"There have been instances of people who were supposedly absent accessing the system, thus indicating that they had shared their username and password "

Per Bengtsson/Shutterstock.com

Don't start with the technology

When all these steps are considered and properly implemented, the project may look at the integration of systems just as an additional phase of the implementation, without worries about the implication from a data integrity standpoint. All in all, the technical solutions should be just the last step in a more extended set of activities, which should start from the process definition, deep analysis, risk assessment and implementation.

If the implementation projects are executed according to a 'top-down' approach, the technical solutions are simply tools that are intended to resolve a specific step in the process. When projects are designed 'bottom-up' (starting from the technical tools), the bigger picture can be missed. The result is a patchwork rather than a clear and simple picture. ■