TONY DAVIES COLUMN

COVID-19 #2: Compliant data processing from your home office

Antony N. Davies[a] and Mohan Cashyap[b]
[a]SERC, Sustainable Environment Research Centre, Faculty of Computing, Engineering and Science, University of South Wales, UK
[bc]MASS Informatics, Harpenden, UK

This column continues our theme of supporting working whilst unable to freely or safely access the analytical laboratory. We want to look at what advances have been made in systems allowing spectroscopic data processing from your home office. This has always caused particular problems for those working in highly regulated environments, such as the pharmaceutical industry, and their supplier and support contractors.

Definitions of Open and Closed systems, blockchain

In general, regulated industries have tried to avoid their IT environments falling into the "Open" category due to the increased requirements to ensure data is not capable of being tampered with. Within a well-protected company network this should not be a problem, as they are classical "Closed" environments under the definition. "Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system." In contrast, cloud provision can fall under the Open system definition. "Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system."[1]

Now, if you refer to the introductory columns on use of Cloud Computing,[2,3] we discussed various types of Cloud systems which were more or less likely to be able to meet compliance criteria. The FDA Open system adds additional burdensome requirements on the IT infrastructure and software solutions, such as encryption of the data (not just when in transit) and full electronic signatures. But the problems don't stop there, as the requirements for full training records for all systems staff to prove they are GxP compliant and up-to-date doesn't vanish when you outsource your IT infrastructure in an Open system… it just transfers the responsibilities to your external host/provider.

The big cloud hosting organisations claim to have regulatory compliant offerings, but if you approach them you need to know exactly what your strategy will be. For regulatory inspectors, the focus is more and more on data integrity. Who has had access to what and what did they do in your compliant environment is key to demonstrating data integrity and that your security features have been correctly installed and are operating fit-for-purpose. Where some cloud providers have issues is in making their system audit trails open for inspection, so this is a key area you, as customer, need to ensure you have what you need.

Advances in blockchain technologies is one area where we may be able to steal innovations driven by other sectors. Our requirements on automated audit trails cover all actions mandated for audit and signoff by our different regulators. These must remain secure even when data moves outside our immediate internal IT environment, a common critical underlying functionality in blockchain systems. Here the chain of data and the audit trail can be proven to be tamper-proof. But to exploit this we need not only better software systems but also improvements in our hardware environments to ensure no data leakage. Things to consider, for example, when allowing remote working include ensuring no password sharing, IP tracking can easily be spoofed if you want to beat the system, so you need better systems to detect data leakage, maybe something like the anomaly detection capabilities used by banks with similar problems.

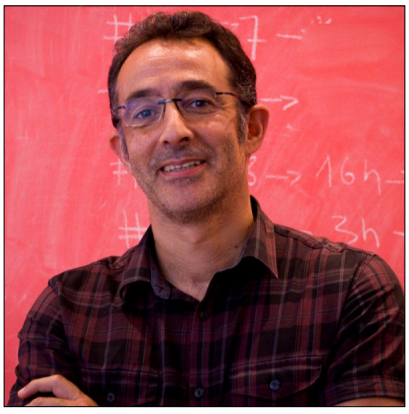
One of the essential tools for ensuring better data integrity is extensive automation of the data transmission and processing functions. This also leads to opportunities to support the work of the Quality Person in a regulated environment through the deployment of some levels of artificial intelligence to support the checking of, for example, study documentation. Scanning documentation for "obvious" or formal errors such as unlikely, incorrect or missing date, out-of-tolerance results, missing fields etc. can easily be automated. This does not replace the work of the Quality Person, but assists them by focusing their work on the anomalies in documentation they would normally have to find themselves. Taking this a step further, you can imagine working on the supporting analytical data and, for example, being able to identify where two spectra were so "identical" as to effectively mean it was impossible that they had come from two

separate QC measurements; thereby flagging possible errors or attempts at fraud.

Deployment examples of compliant cloud solutions

So where are we in terms of moving our systems safely into a cloud environment? Santi Dominguez, CEO of MestreLab, had some interesting comments which also reach back into the previous column[4] on making use of the extra time we have working from home to upskill: they have been running a series of additional free training workshops.[5] They saw that many people taking part were already using their software but were looking for additional training in more advanced spectroscopic data processing in areas they did not currently exploit. After years of this column complaining that the chromatographers are well ahead of the spectroscopists in the advanced level of IT system support with their chromatography data systems (CDS), it was interesting and nice to hear from him a feeling of obligation to develop similar advanced data handling and analytical workflow oriented support for spectroscopists…

"At Mestrelab we have been moving towards allowing our users to work remotely and freeing them from geographical restrictions. We see this access to data anytime from anywhere as being a critical part of the Lab of the Future. The design of our tools and solutions has had this idea at its heart for several years, and we are either there or getting there with most of the tools. The coronavirus pandemic has illustrated this by making remote work compulsory rather than desirable, and the amazing attendance we have had to our COVID19 workshops has shown the interest in the community in the value that this geographical flexibility offers."



Santi Dominguez

With LIMS systems being very much focused on standardised procedures or biased to handling chemical structures at their core, it would be great if spectroscopists would finally have a cloud-based enterprise application to support our work. Santi and his colleagues have taken this on board and are producing a system which can automate large parts of the "request>measure>capture_data>retrieve>process>report>archive" workflows we all use. He commented…

"With the technology available today, there is no reason why you should not be able to continue to progress your research and work just because you are travelling, at a conference or because a global pandemic prevents you from going to your workplace. It is up to us, as solution developers, to allow our users to transcend those geographical limitations, and this is at the core of our philosophy as a company."

We also had a really useful discussion with Heather Longden, a former colleague (of TD) who has a role as Senior Marketing Manager at Waters for Pharmaceutical Regulatory Intelligence, is a specialist in compliance to e-record regulations and an active member of ISPE GAMP Community of Practice, where she is called on as an expert in Data Integrity. In light of the working from home challenges today, Heather acknowledged that the Empower Cloud CDS has been adopted by a number of highly regulated laboratories. As Steve Bird, former Director of Informatics Strategic Marketing included in an Amazon Web Services (AWS) whitepaper...

"Users can sign on to Empower Cloud from any online computer or device, inside or outside of their organisation's network, using the same Empower credentials they would use at their desks or in their laboratories. This change significantly enhances their business continuity and data security capabilities while also ensuring their compliance and validation requirements are met."

Heather was very positive about putting scientific data processing systems into the cloud and had some positive stories where the deployment to the cloud used in an IAAS (Infrastructure as a Service) can actually greatly improve the compliance position of a company. Here I must apologise for citing a CDS system, but it does show what is now possible. Clearly there are additional challenges to solve for SaaS (Software as a Service) applications for regulated laboratories, but the IaaS model allows scientists to run dedicated individual single tenant solution on cloud infrastructure. In Waters' case, they have partnered with AWS as a cloud provider, and leverage automated AWS provided scripts to "install" the application, which is more reliable and consistent than an IT expert deploying applications on inhouse developed, on-premise infrastructure.

Heather did point out that when auditing or verifying your cloud providers understanding and delivery of GxP compliance requirement, be prepared to phrase questions in a way that IT provider's understand, discussing security and authentication, consistent installation etc, rather than IQ, OQ PQ, audit trails and data approval or batch release. Key to this is to ensure that you not only have understood the additional risks, and noting the mitigated risk, but that you also have clear documented agreement laying out who is responsible for what.

"... this is what the cloud provider is responsible for…".

She has been looking at the difference between US and European compliance, which is normally very closely aligned. However, an additional requirement in Annex 11 of the European regulations[6] is to "regularly review" audit trails (and consequently to have documented somewhere that this activity has been carried out).

The annex 11 is not a clear departure from Part 11. It explicitly clarified an expectation of both agencies that ALL critical data and meta data is reviewed.

TONY DAVIES COLUMN

Especially during the pandemic, a compliance trap has opened up with vendors being supportive by making additional licenses of their products available to people working from home. Although it might be obvious, just because the software is the same release version as what you have installed on your desktop computer in your laboratory, it will still need to be a validated installation on a validated computer system. So beware of trying to install your scientific data processing software onto the family's ultra-fast gaming PC… you might produce those 2-million datapoint surface plots really quickly, but you will not be able to use the results in a compliant manner!

I would like to finish off with an example Heather cited of the use of the cloud, not just to reduce costs in your IT environment but to exploit it to produce a much stronger compliant position where companies are working with external third parties such as contract research organisations (CROs) or contract manufacturing organisations (CMOs). Here, the contracting organisation uses an IaaS cloud deployment of their own to be the SaaS provider to their subcontracting CROs and CMOs (Figure 1). This reduces the worries about setting up and ensuring rock-solid Chinese walls with your subcontractors especially around data leakage.

Essentially, the subcontractors are carrying out the work for the contracting company in their own laboratories, but the instrumentation is run through the cloud software deployment of the contracting organisation. Again, a clear case where everything must be very well documented, but does eliminate many of the compliance hurdles associated with out-sourcing much of your new product development activities while maintaining an overall strong compliance position. Waters have a funny short video explaining all this much better than we can, which I would recommend watching if you have a spare four minutes.[7]

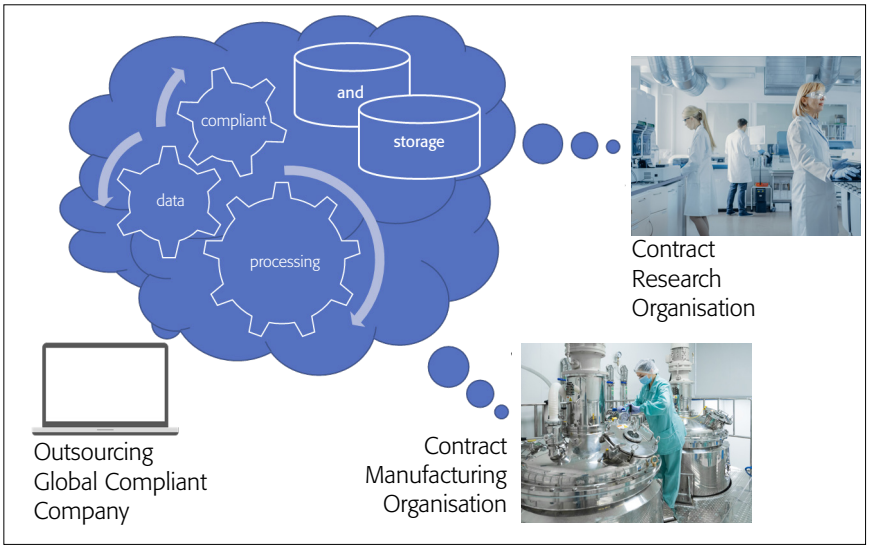


Figure 1. CxO organisations creating data which is acquired directly into the cloud-hosted enterprise application and owned by the outsourcing company.

Conclusions

So, thankfully, it seems that we, as a community, have moved substantially forward since our earlier articles on the introduction of cloud-based solutions. The solutions have addressed the compliance issues and seem to have started to actually deliver more flexible enhanced compliance positions over conventional deployments. If you have any good examples of such innovation yourself, please let us know and we will see if we can feature them in future columns.

Thanks!

Special thanks to Heather Longden at Waters and Santiago Dominguez at MestreLab for some very useful discussions and inspiration when putting this column together!

References

1. *Electronic Code of Federal Regulations, Title 21: Food and Drugs, Part 11—Electronic Records; Electronic Signatures*, e-CFR data is current as of 14 May 2020. https://www.ecfr.gov/cgi-bin/text-idx?SID=10b1b35c3a3ca71cf54d46dde50ab704&mc=true&node=pt21.1.11&rgn=div5
2. A.N. Davies and M. Cashyap, "A head in the clouds?—Part one", *Spectroscopy Europe* **26(3),** 21–22 (2014). https://www.spectroscopyeurope.com/td-column/head-clouds-part-one
3. A.N. Davies and M. Cashyap, "Who's ahead in the clouds?—Part three", *Spectroscopy Europe* **27(1),** 18–21 (2015). https://www.spectroscopyeurope.com/td-column/whos-ahead-cloud-part-three
4. A.N. Davies and H.-J. van Manen, "COVID-19: Lock-down and up-skill", *Spectroscopy Europe* **30(2),** 19–21 (2020). https://www.spectroscopyeurope.com/td-column/covid-19-lock-down-and-skill
5. COVID-19 Mestrelab workshops: https://resources.mestrelab.com/webinars/
6. EudraLex, *The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use*. Annex 11: Computerised Systems (2010). https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-4/annex11_01-2011_en.pdf
7. https://www.waters.com/waters/en_US/Empower-Cloud-with-AWS/nav.htm?locale=101&cid=134950285