Emerging Challenges for Data Integrity in the Pharmaceutical Sector

Processing power has completely reshaped manufacturing over the last 20 years, especially in pharmaceutical production. Businesses can now monitor, analyse and model far more data than ever before, which has led to significant advances in drug discovery and development. Automated machinery has also allowed production to expand at an unprecedented scale giving more people greater access to the medicines they need.

Running in parallel to this progress, however, has been a growing threat to data integrity – the foundation on which businesses in this sector maintain their reputations and develop new opportunities. The previous two decades are arguably defined as much by regulatory oversights and human error as they are by technical progress. In 2019, for example, the US Food and Drug Administration (FDA) issued over 90 warning letters, extending a pattern of failures that can be seen across the pre-market side of the industry since the turn of the millennium.

In most cases, warnings are given for similar reasons. One study that analysed FDA letters in the US between 2007–2018 found that most were issued for failing to follow and maintain correct procedures or poor documentation practices. The same study concluded that cases of required action were on the wane, and a growing number of businesses were compliant with stricter industry guidance. This is clearly positive news but also a situation that cannot be expected to remain unchanged. Data integrity is an ongoing process, rather than a static state, and requires businesses to be aware of potential threats ahead of production.

What is Data Integrity and Why is it Important?
Data integrity is relatively easy to define but difficult to manage. Businesses across the sector are expected to follow guidance, including companies responsible for clinical trials, research, manufacturing and distribution. Any information generated must be complete, accurate and consistent without any deviation from prescribed methods set out in guidance. It should also be collected, stored and maintained using secure methods.

The acronym ‘ALCOA’ can be used to better understand what’s required from businesses. It stipulates that all data should be attributable, legible, contemporary, original and accurate. Beyond this, there’s an expectation that data should be accessible at all times, particularly because auditors can arrive with little notice.

There are countless decisions made each day in drug manufacturing facilities, all of which can directly impact human health. Data integrity procedures are ultimately there to ensure a company is producing a consistently high-quality product. Those with accurate information have the means to demonstrate good practice and can quickly
Historical Challenges

Good data integrity processes ultimately build trust between industry and regulatory bodies while also helping to limit the chances of product recalls, compliance issues and damage to a business’s reputation. This idea is best seen in a lawsuit from 2018, which saw Fresenius SE canceling its $4.3 billion acquisition of US drugmaker Akorn Inc. Fresenius claims that Akorn did not have sufficient controls in place to guarantee the reliability and validity of data gathered during process development for one of its products. Once a judge ruled that Fresenius’s withdrawal was justified, Akorn’s shares dropped by 59%.

Fresenius vs Akorn is exceptional because it scuppered a significant acquisition, but the conditions which caused the deal to be called off are not unusual. Indeed, data integrity and validation continue to be a problem for many organisations in the sector, not least because ‘hybrid’ systems that exist half on paper and half digitally are still relatively common. The World Health Organization’s latest guidelines discourages the use of these systems, and says migrating to a completely digital set up should now be prioritised.

Such moves, however, are perceived to be difficult and time-consuming. A typical facility will have many machines that generate data, usually developed by different companies using different recording techniques. Many machines will not come with software. Those that do will require validation – a systematic approach required to guarantee that any process in a pharmaceutical facility will operate within specific parameters when required. This process can take months to complete depending on the experience of those carrying out the validation and whether they are following specific procedures.

Some organisations offer integration of all instruments, but this usually falls short of ALCOA requirements and can actually drag out the process as individual assessments of each connection need to be tested. Standardised software solutions are seen to be the preferred way to digitise paper-based approaches as they are tested more rigorously and simplify the validation process, even when connecting multiple machines and instruments.

Businesses have also had to contend with a complex regulatory landscape that continues to shift. To combat the spike in compliance failings, the World Health Organization, UK Medicines and Healthcare Products Regulatory Agency (MHRA) and US Food and Drug Administration (FDA) have all issued draft guidance for maintaining data integrity. For manufacturers, these updates run alongside other requirements, such as GAMP-5 issued by the International Society for Pharmaceutical Engineering, which defines good practice when using automated systems in the sector.

Emerging Problems

While the move from hybrid systems is welcomed by regulators, businesses are still being flagged for data integrity shortcomings even when using newer digital systems. One of the biggest challenges that has emerged over the last twenty years relates to audit trails, particularly among companies that use software with audit trail functionality. There is a tendency to fit and forget without
revisiting the data and understanding what’s being collected and why. This can pose challenges when work is being submitted to a quality group for review.

The age of some automated systems is another critical concern, particularly for drug manufacturers. As equipment reaches a certain age, hardware and software components inevitably fail or become obsolete – this not only jeopardises the validity of some data but also the required quality of a product. However, major retrofitting projects come with their own risks, and business owners are advised to proactively manage their systems to identify when components need replacing. This approach limits plant downtime and ultimately protects data validity, even as processing changes are made.

**Access Privileges**

Digital systems adhering to good manufacturing practices will use strict controls to maintain the reliability and integrity of data. This includes procedural controls, technical checks and audit trail reviews. However, many organisations fail to account for the risks associated with privileged access. This essentially grants someone the power to carry out critical administrative tasks, such as issue resolution or a change in monitoring parameters, often without traceability. Unsurprisingly, this situation is not viewed kindly by auditors as it violates one of the ALCOA principles – namely, that data should be attributable.

While privileged access does not compromise a system per se, guidance is nevertheless clear that facilities should avoid reliance on so-called ‘God accounts’ with minimal limitations. It significantly raises the chances of human error that could lead to falsification or data falling out of specification, not to mention give disgruntled employees or inside actors the opportunity to purposely do damage. The latter may be an extreme example but cannot be discounted in an industry known for placing high pressure on teams to produce positive outcomes for influential clients.

The solution here is to avoid using a single administrator account by splitting privileges between the IT and OT domains. This ensures one person is responsible for users and the types of data they can access, and another for the instruments and information collated on the plant floor. These individuals can then apply principles of least privilege to users in different business areas – e.g. providing users with the minimum access they need to their work for the minimum time required.

Legacy systems will not have admin splitting features built into their design, and it’s difficult to retrofit a solution. Fortunately, modern data acquisition systems make this process far easier as they can slot into a facility’s existing infrastructure, allowing older equipment to continue in operation without extensive changes or validation required.

**The Problem with Big Data**

The sheer growth of data presents another critical challenge. Thirty years ago, most drug manufacturing facilities would have used a paper-based recorder to monitor temperature and pressure, with a limited number of lines plotted on a chart. Colleagues would then measure this information against a template to ensure processes fell within set parameters. Today’s acquisition systems, however, can gather a vast range of different inputs and outputs, including flow, inlet or outlet conditions, packing and other critical environmental data. While these spreadsheets are suitable for research purposes, it also means there is a higher chance of data falling out of specification. Consequently, manufacturers now have to be sure all this extra information is calibrated correctly; otherwise, large quantities of the product may need disposing.

Long, unstructured data sets also create added pressures for the audit trail and those responsible for them. At one time, these records were designed around significant changes like a colleague signing in to begin a batch or someone changing an alarm. However, every action must now
be recorded, including the transfer of files across an organisation’s internal network. These small additions mean it now takes much longer to check a batch, increasing labour costs and the chances of disruption.

At one time, auditors only required notes of significant changes, such as a colleague signing in to change an alarm. However, updated guidance seen in ‘21 CFR Part 11 Electronic Records; Electronic Signatures – Scope and Application’ now force colleagues to go through an audit trail to corroborate every change that has occurred during the production of a batch, no matter how inconsequential.

This level of detail is undeniably good for robust data collection. On the other hand, updates to guidance can significantly impact a plant’s competitiveness, increasing the time needed to check a product. It will also drag out the investigation process should an error be flagged.

One way through this problem is by adopting systems that request a reason for change. Date and time stamps have long been part of audit trails, as have user accounts, but a clear way to explain colleagues’ actions has been lacking. A high-temperature alarm on a freezer, for example, may go off during production because someone left the door open too long. Traditional approaches to data acquisition would log this event in the audit trail but not offer any extra information. This makes the prospect of identifying and eliminating possible issues far more complex.

Newer modular systems that offer a more controlled summary of events, however, will help to speed up checks and encourage a more diligent approach to data integrity. Users that enter a dash or full stop in one of the entry boxes would soon be identified, encouraging them to provide a more complete explanation the next time they are prompted.

Culturing Compliance
Engineering systems and ensuring they’re compliant can often cost more than specialist instruments used to create products. Manufacturers need to know their programmable logic controllers are working correctly, but they also need to be sure the information collected by a SCADA system is accurate and reliable. This issue only gets more complex when businesses opt for proprietary systems with a high GAMP level, as this will require extensive validation work that can take months. Worse still, the entire procedure will need repeating if problems are found or new functions are added later, making it harder to complete.

The cost of meeting data integrity requirements is considerable, and for some, the risk of penalties will be offset by not investing in new equipment. Yet this attitude has been shown to have far-reaching complications, hitting share prices and big name reputations. Those more risk-averse may opt for cheaper systems, though these can prove a false economy when ongoing validation work drives up the overall cost.

So-called ‘off the shelf’ packages seem to offer the best of both worlds, allowing a business to quickly scale up without losing sight of its data. Though no system is ever infallible, and data integrity has as much to do with culture as it does with technology, products of this type offer a cost-effective route to compliance. This is invaluable in a time where there is a marked rise in the number of health authority enforcement actions – some of which have the potential to close doors permanently.

These are just some of today’s challenges and opportunities for data integrity in drug manufacturing. It could be argued that some of the measures discussed are unnecessary, especially given how compliance appears to be improving over time. That said, it would not be outlandish to suggest that guidance will soon become law. As such, it would be prudent for organisations to move towards more adaptable systems that promote best practices without significant disruption.

Peter Cusworth is Industry Development Manager for Yokogawa’s Controls and Instrumentation Division. Throughout the last 20 years, he has worked closely with the industry’s most recognisable names to engineer systems that improve production while also promoting best practice around data acquisition and control. Peter has been central to the development of Yokogawa’s SMARTDAC+, a GX/GP paperless recording platform that has been designed to tackle data integrity challenges in research, development and production environments.