Awareness And Precision Are Key To Manufacturing Data Integrity

Data sits at the heart of the pharmaceutical-product equation. The huge volume of data generated in drug discovery and development, and to provide support for regulatory approvals, is only the start. Increasingly, data flows from post-approval safety requirements, drug manufacturing, predicting and tracking health outcomes, or communicating with a wide range of stakeholders.

In today's industry, data is arguably the product. Ensuring data integrity proactively at every stage of the product lifecycle is therefore paramount if pharmaceutical companies are to maintain their reputation, competitive edge and financial stability, as well as the safety and trust of patients. Compliance failures have a long tail in an environment where risks and benefits are always in delicate balance.

This applies especially to the manufacturing processes that set-in motion the pharmaceutical supply chain, more so as drug manufacturing becomes increasingly complex in line with the market trend towards biologics, biosimilars and gene therapies. At the same time, globalization of manufacturing networks, whether for reasons of cost efficiency or market access, has raised concerns about the challenges of maintaining quality standards from a distance.

Recent years have witnessed sharp increases in costly and disruptive product recalls, delayed approvals, import bans and other sanctions due to lapses in data compliance identified during GMP inspections. These may result from technical malfunctions or human error; lax documentation practices; systems, equipment, standards or testing methods that take insufficient account of data integrity; or inadequate data review, quality assurance and oversight.

Regulators in key markets are also making clear that issues of data integrity go well beyond what happens in drug laboratories or clinical trials. Just as widespread computerization has migrated from these settings to manufacturing facilities, so the risks of data integrity lapses in drug production have multiplied.

Potential New Point Of Emphasis

A potential new point of inspectional emphasis may be signalled by the recent issuance of regulatory-agency inspectional observations broadly citing firms for failure to maintain 21 CFR Part 11 compliance in areas beyond the laboratory.

Issued by the FDA in 1997, the 21 CFR Part 11 final rule set out the federal requirements for electronic records and signatures in FDA-regulated industries. The recent message seems to be plain: all other aspects of the pharmaceutical enterprise that rely on computerized systems will be expected to be as fully compliant with 21 CFR Part 11 as quality-laboratory or clinical-development activities.

This recent sharper focus on data integrity 'beyond the laboratory' means taking lessons learned from existing Part 11 compliance programs and applying them with equal rigor to pharmaceutical production equipment and enterprise resource planning (ERP) systems, as well as Building Management Systems (BMS), and preventative maintenance/calibration systems for manufacturing equipment.

The regulations call for managed access to the data generated and stored by these systems. In the case of BMS, the temperature and humidity data often stored by these systems should be accessible to facilitate investigations in the event of temperature and humidity excursions. Moreover, the data must be readily available to demonstrate that temperature-sensitive materials were handled, stored and tested under conditions consistent with a product's labeling requirements.

Whereas the consequences of data-integrity lapses in these circumstances may seem minor, environmental controls are closely monitored for a reason. Sub-optimal storage conditions can potentially affect the purity and effectiveness of the drug product and associated raw materials, such as the active pharmaceutical ingredients, certain excipients and even empty gelatin capsules.

Body Of Guidance

There is now a growing body of guidance on data integrity from regulatory agencies and organizations such as the US FDA, the Medicines & Healthcare Products Regulatory Agency in the UK, Australia's Therapeutic Goods Administration and the Pharmaceutical Inspection Co-operation Scheme.

Data-integrity requirements span a broad spectrum of activities and environments, all under the umbrella principle of ALCOA: that data must be Attributable (who performed the activity and when?); Legible (is the data readable/understandable?); Contemporaneous (recorded at the time of the activity?); Original (an original record or certified true copy?); and Accurate (error-free?).

In line with the broader regulatory-agency scrutiny noted above, these regulations and guidance underline that data integrity in pharmaceutical manufacturing is now expected to be subject to the same levels of control and scrutiny as the laboratory or clinical settings.

That calls for a pro-active, long-term holistic approach that incorporates the lessons learned from activities taken to ensure the integrity of data in the pharmaceutical laboratory. Companies must apply, on a broad scale, the detailed guidance from global regulatory authorities, creating and resourcing data-integrity governance systems and action plans to ensure that data are recorded and monitored as accurately and consistently as possible at every stage of the pharmaceutical endeavor.

Crucially, companies must have in place a well thought-out and understandable Data Governance program. When pharmaceutical regulatory-authority inspectors have found no evidence of a documented Data Governance program, inspectional observations have followed.

Cultural Failings

Deliberate misrepresentation, falsification, manipulation, omission or deletion of data constitute fraud subject to criminal sanctions. More often, though, data-integrity issues reflect failings in corporate culture or simple lack of awareness. Even when lessons are learned in the laboratory or clinical development, they may not always be carried forward into other areas. It is far from clear that the pharmaceutical industry fully appreciates the need to apply the 21 CFR Part 11 requirements and ALCOA principles to computerized systems 'beyond the laboratory', including manufacturing and facilities systems.

Companies must recognize that apparently simple oversights that stem largely from poor or sloppy practices, rather than fraudulent activities – such as transcription errors (Accurate record?); discarding hard-copy records which are later realized to be original records (Accurate or Original record?); taking notes in personal notebooks (Original or Contemporaneous record?); or illegible signatures/handwriting (potentially violating both the 'A' and 'L' ALCOA principles) – can, and do, lead to serious data-integrity issues.

Managing work culture, and embedding quality and diligence in that culture, are fundamental to maintaining data-integrity standards in drug manufacturing. A clear link must be made between quality and outcomes of concern both to the business and the patients it ultimately serves.

Companies should also have a full understanding of how and why human errors – or, in the worst case, deliberate manipulation or falsification of data – occur and the psychological drivers for non-compliance. If employees feel under intolerable pressure at work, for example, they may be tempted to use that pressure as a rationalization for sloppiness or even willful misconduct.

Computerized Manufacturing

Part of the challenge lies in the pace of technological change. Throughout the 1980s and into the early 1990s, the operation of pharmaceutical manufacturing equipment remained largely manual. By contrast, today's manufacturing systems are heavily computerized, capturing huge volumes of data and often maintaining detailed audit trails.

Modern computerized production equipment frequently has the capability to store programmed 'recipes' that control the equipment's operation so that it generates a specific product. Access to these recipes must be tightly controlled, in line with both ALCOA and change-control principles.

Too often the scale of data generation in manufacturing and its implications for compliance are poorly understood. Plants may lack basic practices and procedures to ensure data integrity outside the laboratory, as well as effective higher-level data governance systems to guide the creation and day-to-day conduct of applicable practices and procedures in relation to data generation and protection in these areas.

Regulatory agencies have cited manufacturing equipment with automated control systems for lack of time-stamped audit trails, data-management systems, alarm-management systems and data-archive and -retrieval systems. All of these manufacturing equipment-related systems have parallels with existing systems used in the pharmaceutical-laboratory setting.

As far as audit trails go, the FDA has recommended in podium presentations made at industry conferences that where these trails are capturing changes to critical data, each record should be reviewed prior to final approval. Audit trails subject to regular review should include changes to: the history of

finished product-test results; sample-run sequences; sample identification; and critical process parameters. More generally, the FDA advises manufacturing facilities to schedule routine audit-trail reviews based on the complexity of the system involved and its intended use.

Trouble With Access Control

At times there seems to be a critical lack of awareness of how the ALCOA principles relate to day-to-day operations in the pharmaceutical-manufacturing environment. For example, if manufacturing equipment is not capable of accepting discrete log-ins from every operator authorized to use the equipment, then a company has a potential data- integrity problem around attributing (the 'A' in ALCOA) an activity to whoever performed it and when.

The issue is the same where operators can share log-ins and passwords for remote computerized control systems that operate manufacturing equipment. Regulatory agencies have indicated that they expect companies to maintain a list of all individuals authorized to use any piece of GMP equipment or instrumentation. The list must also detail each user's access privileges in terms of operating the equipment (again, the 'A' in ALCOA).

As far as the originality of data and records is concerned (the 'O' in ALCOA), if a company is unaware of the extent of data saved by the manufacturing equipment, the paper record may not be complete or even a true original record. Once more, this awareness of the data acquired and stored by modern pharmaceutical manufacturing equipment, and the need to secure and manage those data properly, has significant implications for data integrity.

One such case study was highlighted at a Society of Quality Assurance Annual Meeting in March 2017 by Sarah Barkow and Karen Takahashi from the FDA's Center for Drug Evaluation and Research.

As Barkow and Takahashi explained, a warning letter was sent out to a facility where no passwords were required to log into electronic data systems, and anyone who accessed the system had full software-administrator privileges. An analyst also told FDA inspectors that someone else had used their login to delete and modify data.

Nip It In The Bud

Addressing these issues proactively through training, governance policies, clear protocols and compliance audits will help companies to nip data-integrity problems in the bud, before they escalate into expensive and time-consuming remediation with potential reverberations across the company, its supply chain, shareholders and customer base.

Part of this is about making sure that personnel are suitably qualified to manage processes that involve maintaining data integrity, and that data-integrity remains front of mind in the day-to-day activities of the workforce. The FDA recommends, for example, that staff are trained in detecting data-integrity issues as part of a routine cGMP training program.

"Less dramatic events, such as faulty data entry or programming, can also trigger a chain of events that result in a serious production error and the possible distribution of an adulterated product."

— FDA

These challenges are not unique to the digital era. Data-integrity principles from the age of paper and manually operated equipment still apply, such as ensuring under FDA regulations that backup data are exact, complete and secure from alteration, deterioration or loss; or documenting certain activities at the time of performance.

All the same, computerized manufacturing facilities have increased both the flow and density of data and, under the rubric of streamlined efficiency, multiplied the risks of data-integrity lapses that can have a serious impact on the continuing viability of production facilities.

Whether systems are computerized or not, the human factor remains paramount. The FDA was already sounding a warning in January 1995, when it published a final rule amending certain cGMP requirements for finished pharmaceuticals in the Federal Register[1]. Acknowledging the risk of critical data loss from computer malfunctions in a modern manufacturing environment, the agency stated: "Less dramatic events, such as faulty data entry or programming, can also trigger a chain of events that result in a serious production error and the possible distribution of an adulterated product".

So, while increasingly sophisticated system safeguards and computerized monitoring of essential equipment and programs helped to protect data, the FDA stressed, "no automated system exists that can completely substitute for human oversight and supervision"[2].

Pharmaceutical companies would do well to heed that advice. If they want to prevent causal omissions from spiraling into a full-blown crisis, they must be absolutely sure that data is properly handled, logged and validated at every step of the manufacturing process.

1. Food and Drug Administration. Current Good Manufacturing Practice in Manufacturing, Processing, Packing, or Holding of Drugs; Amendment of Certain Requirements for Finished Pharmaceuticals. Federal Register Volume 60, Number 13. 20 January 1995. Retrieved from https://www.gpo.gov/fdsys/pkg/FR-1995-01-20/html/95-1361.htm.

2. Ibid.

Lachman CONSULTANTS