How to Avoid Data Integrity Disasters In Your Manufacturing Network

Pharmaceutical manufacturers can establish a competitive advantage by preventing questions about the integrity of their product quality data from disrupting current and future revenue, says Lachman Consultants.

In recent years, data integrity shortcomings identified during GMP inspections have cost firms dearly. In some cases, the financial impact has run into the hundreds of millions of dollars. Some of the effects are immediate, while others linger for years.

Despite the risk, many manufacturers generally do not seek help with data integrity compliance until after there's a problem, when it may be too late to avoid an impact on profitability.

For this reason, the Westbury, N.Y., consulting firm urges pharmaceutical companies to establish a competitive advantage simply by taking a proactive approach to data integrity assurance.

A Secret Ingredient for Success

The problem of poor data integrity "isn't just about computers and it isn't just about non-US sites," Lachman's Jim Davidson explained in an interview.

Rather, he said, data integrity control is about revenues and growth. "Because it's the data that allows you to release product into the marketplace, and it's the data that gets you approval from regulatory agencies, it's fundamental to your ability to stay in business and to your ability to grow your business."

It's important for corporate executives to recognize the importance of data integrity to profitability, Davidson said. "You can't expect all CEOs of major companies to have an in-depth understanding of what's going on in some computer system in a lab somewhere, but they need to understand the impact it can have on their business."

The Problem of Delayed Market Entry

The cost of remediating data integrity issues, while typically higher than that of preventing them, pales in comparison to the consequences in terms of delayed market entry.

When regulatory investigators inform a plant manager or senior quality executive that they no longer trust the integrity of the plant's quality data, there are certainly impacts on the plant's quality unit in terms of fixing the problem.

But once the agency's trust has been lost, other far more serious repercussions may come into play.

First, there is the question of whether the plant can continue distributing products with potential quality issues into the US market. If the plant is in another country FDA can decide to add it to the agency's drug GMP import alert, immediately cutting off a revenue stream.

Second, there is the question of whether the agency will approve any pending new drug applications for drugs the company intends to manufacture at the facility.

It is not uncommon for serious data integrity findings to result in a suspension of such ANDA reviews until the problems are cleared up.

Third, the agency can respond to serious data integrity problems by issuing a warning letter to the firm. Such letters warn of potential legal consequences and can undermine the confidence of customers, business partners and investors.

The Problem of Close-Out Delays

Once sanctions have been imposed and a company begins the remediation process, a great deal of time can pass by before an FDA re-inspection of the facility can occur. As a result, a company's financial prospects can be significantly impaired due to delays in closing out warning letters, lifting import bans and approving applications.

Lachman estimates that, on average, it takes at least a year to resolve issues raised in a Form 483 report. Although there are cases where it has taken as little as six months, it frequently takes as much as two years. And when there is a warning letter, it can take even longer.

Unfortunately, during these delays, companies often must revise their revenue projections. They may find that during the hiatus, a first-to-file ANDA may have drifted back into a distant also-ran, which would translate into far less revenue potential for the firm.

Even after market removals due to warning letters or other regulatory deficiency notices are resolved, they can cast a long shadow over long-term future profitability, Lachman says.

The problem is that these developments constrain firms' strategic options. Because they're late to market, they must charge less. Meanwhile, they can face an increased cost of capital and reduced market capitalization. Plus, distrust among their employees and customers can make it harder to do business.

For these reasons, Lachman said in a recent whitepaper that data integrity issues "are fast becoming the biggest threat to profitability for the pharmaceutical manufacturer, particularly generics."

The Real Cost of Poor Data Integrity

In a recent analysis, Lachman tallied the real cost of poor data integrity based on actual cases, and found that it was stunningly high.

In one case that Lachman researched, data integrity problems found on inspection led FDA to send a warning letter to a global manufacturer in January 2015, and ban US imports from two of its facilities in March of that year.

Exports, which had grown 39% over the previous four years, fell by $48 million.

Meanwhile, the firm spent an estimated $40 million to $70 million on remediation and write-downs.

Additionally, 41 generic drug applications and 38 drug master files were in jeopardy.

A Billion-Dollar Fiasco

In another case, a large manufacturer based in India fared even worse, with a data integrity situation that Lachman figures will wind up costing it nearly a billion dollars.

This company's problems started with an FDA import alert in early 2013. Then the UK Medicines and Healthcare Regulatory Agency required the recall of multiple products, and in late 2013 FDA issued a second import alert covering all active pharmaceutical ingredients. The company recalled all products in 2015.

During this period, the firm's US revenues fell from 50% to just 24% of total revenues, for an expected revenue loss of $760 million.

Write-offs and remediation expenses in this case are expected to exceed $100 million.

Additionally, the firm saw a loss in market capitalization of $2.3 billion.

A Painful Statistic

Given the high cost of poor data integrity, one might think that most of the world's thousand-plus generic drug firms would make sure they achieve sustained compliance in this area. But the reality is many do not, Lachman says in its whitepaper. "Our experience tells us that the number is painfully low."

Despite the benefits of the proactive approach to data integrity compliance, many firms don't seek help until they're already in trouble with the authorities.

That means they're in for a painful process.

"We'll come in with a team of people," Davidson said. The team will start going through data "to look at what impact the lack of controls has on the data itself for product in the marketplace, because that's what FDA is concerned about the most."

Lachman uses a statistical approach it has refined over the past few years to evaluate product lots that are already on the market, released based on data that have since become suspect.

It's an intrusive, disruptive process that consulting firms like Lachman will undertake to carry out these assessments, he said. It involves reviewing not just the electronic data but also the paper records for each batch.

If it's a firm outside the US, FDA may have imposed an import alert, Davidson said. "Now you can't export to the U.S. market anymore and if that was a big part of your business, that's a big loss."

However, the firm may still be trying to produce for the rest of the world, he said, "but you've got people like me and other consultants in your facility reviewing your data and interviewing your people in order to determine whether there are issues that impact the product's ability to remain on the market or not. This results in a need to commit significant internal time and human resources to support the independent data review."

When Good Product Can Have Bad Data

Even if FDA finds a lack of data integrity, it doesn't automatically mean there's a quality or purity problem with the drug product.

For example, there have been cases where FDA found that laboratory technicians were weighing samples far more quickly than possible, revealed by reviewing weight tapes with time and date stamps, and concluded on this basis that they were likely replicating the same weight over and over again.

Although such a determination means the exact weight of the samples is unknown, "sometimes it doesn't end up impacting

the data in a meaningful way because the difference of that is a tenth of a milligram. But still, the data has been 'falsified.'"

It's up to the company, often with the help of outside consultants, to prove to the agency that there is no impact to the quality of the product. Davidson indicated that this can often be done by considering the totality of the data associated with a particular batch of product.

When Lachman responds to for-cause findings, "it's almost an emergency situation where you're trying to gather enough information to show that despite the issues uncovered by the regulatory investigator, the product in the market doesn't pose a risk to quality and efficacy of the products."

Original Records Sin

Because the most highly publicized cases involve fraud allegations, many people have the mistaken impression that if their team is honest and ethical, they won't have a problem with data integrity. But such is not necessarily the case.

"Most people think it's fraud and in the overwhelming cases it's not," Davidson said. "There are instances where it is, but the overwhelming majority of the things we've investigated are data being compromised by sloppy practices and things of that sort."

It can result from poor systems design that stems from rapid growth. A company that starts out with one site and suddenly has five sites in several countries may not be prepared for the resulting management challenges. "The control piece can often get away from companies, and we certainly see that," Davidson said.

He noted that today's data integrity crisis echoes the US generic drug scandal of the late 1980s and early 1990s, when there would be what he calls "old school" data integrity failures. "One of the reasons for the keen interest by the regulators is they're intent on it not happening again."

Back then, firms were accused of fabricating records of equipment they didn't have, or substituting overcoated innovator tablets for bioequivalence testing.

But today's data integrity lapses differ, tending to revolve around computer records, and sometimes involving confusion about the regulatory guidance that has proliferated around this issue, Davidson said. "There are expectations out there in terms of guidance, but firms need to determine how best to implement the guidance procedurally at their firm."

"In some parts of the world where the industry is growing very quickly there just aren't these mid-level or frontline manager and director level people that are keeping track of what everybody is doing every day."

— Jim Davidson

One area of confusion that often arises is around the concept of original records. People will print documents from an electronic system and treat them as original records like they used to do with paper-based systems. But they're not. "If there's a computer involved in generating the paper, then the electronic data that resides on the computer is the original data from the regulator's perspective," Davidson explained.

Some regulatory agency investigators have learned how to "go in and look at live data on ... companies' systems and seeing what's there," Davidson said. "That's been a big change since 2013 when the recent trend of data integrity observations really began to get noticed."

Crazy Quilt Guilt

Much of the focus of recent inspections has been on software in chromatography systems used for batch release testing.

The software in these testing systems uses a folder/file structure that's much like the one in Microsoft Windows computers.

As with any group of computer users, there will be a tendency in the analytical laboratory for each user to organize the file folders in shared equipment based on individual preference.

If "they're allowed to set up folders willy-nilly just any way they want and name them any way they want ... and that happens a lot ... the ability to go back in and find specific data becomes almost impossible."

Regulatory agency investigators will look in these chromatography systems during inspections, and "if they see a crazy quilt of folders in these systems ... what happens is they don't bother digging around in those folders and proving that there's a data integrity issue. They just say that the conditions exist and are likely to cause a data integrity issue."

Then it's up to the firm to prove a negative, to show that the data are still intact as originally generated.

That can be straightforward with a well-organized file structure, but difficult if not impossible with a poorly controlled, poorly organized crazy quilt structure.

The Importance of Data Governance

A key factor in ensuring data integrity is to establish a data integrity governance policy as discussed in regulatory guidance from MHRA, FDA and other regulatory authorities.

Putting this policy into place is more important at the outset than "worrying ... about the detailed specifics of how I'm going

to do the things that are laid out in the data integrity guidance documents," Davidson said.

Once they have a data integrity governance policy, firms should develop the detailed procedures supporting the policy and periodically conduct internal audits to review compliance or rely on external auditing if they lack the expertise.

When firms have done this work up front and alerted FDA "that you've looked at the systems when they come in, you're looking at the systems, you're getting your house in order, and we've seen in some cases forbearance by the regulators."

When a firm has a plan with dates and commitments for addressing data integrity risks, regulatory authorities are more likely to let the firm continue with its own remediation.

"If you're in control of it yourself, it's a much easier thing than having to do it at the behest of the regulatory agency," Davidson observed.

The Need to Hire the Right People

Right up there with establishing a data integrity governance policy is ensuring that the organization has people who can ensure that there are enough controls in place.

There is a tendency at firms to focus on strengthening data integrity by acquiring new information technology systems. But someone must know how to use them.

"We have worked with firms that bought IT data management systems that are the gold standard," Davidson said. "But then when they install them they don't install them properly."

Another personnel challenge that gets firms into trouble on data integrity is a shortage of managers.

"In some parts of the world where the industry is growing very quickly there just aren't these mid-level or frontline manager and director level people that are keeping track of what everybody is doing every day."

When workers don't know how to do something, there's no one to ask. And when they don't realize they need to ask, there's no one who will see they need help.

"In places where they probably need it most there's the least number of those kinds of people to find and hire," Davidson said.

The Perils of Password Sharing

Another issue is a tendency of workers to circumvent GMP controls, for example by sharing passwords to equipment such as analytical instruments.

A fundamental GMP requirement is to "attribute everything that's done to an individual and when they did it, when they took a particular action, did a specific operation, operated a certain instrument."

Even if the data generated with the equipment are good, sharing user names and passwords prevents the authentication required, Davidson said. "It's a GMP issue that leads to potential data integrity issues because you can't attribute the data to the person that actually did the work."

Plus, if the data are bad, password sharing makes the problem difficult to investigate. If you don't know who made the mistake, you can't ask them how it happened.

Integrity Can't Be Outsourced

It's not unusual for FDA to find data integrity issues at firms that have been audited regularly by pharmaceutical companies that use them for contract manufacturing or testing.

The firms will often ask the consultant they've retained to deal with the issues FDA uncovered why their customers' auditors or their own internal or third party auditors didn't identify the problems. Davidson said that in many cases, the internal or external organizations that conduct these audits may lack sufficient expertise in terms of auditing to detect data integrity issues. In certain other cases, practices that put data integrity at risk are so deeply embedded (intentionally or unintentionally) in firms' systems that they are difficult to detect during a short term audit.

This is an important problem, because FDA and international regulatory authorities hold pharmaceutical companies responsible for the quality and data integrity of the work they outsource.

The Need for a Holistic Approach

Although firms tend to focus on computer systems when troubleshooting data integrity issues, Davidson said Lachman takes a different approach. "We think it has to be done holistically."

"You have to look at how the computers and computer systems are being used by the people, the lab people or the manufacturing people that are actually touching them."

For example, workers can save production routines in tablet compression machines that govern factors such as speed. But if the company doesn't control access to that software, any worker could come along and change the routines.

In other cases, software limits the number of user name/password pairs a production machine will accept. If it allows 10 passwords but 30 workers need to use it, then there is going to be password sharing – and it will be impossible to tell who was using the production machine when a deviation from required practices occurs.

A Better Way

In the end, those who view quality as an investment rather than a cost do best on data integrity, Lachman emphasizes in its white paper. "This requires a mindset shift away from being a victim of the winds of regulatory demands to proactively seeking the source of quality deficiencies."

Rather than brace for expensive surprises like recalls, import bans and loss of reputation, Davidson said it's so much better to incorporate activities like proactive data integrity focused auditing into your budget and schedule. Whether done internally or with the help of an outside firm, it can be so much more effective than waiting to find out what the regulator sees and hoping for the best.

Lachman
CONSULTANTS