



**Data Integrity:  
A Multifaceted Commitment of Quality**

When you consider data used by companies to make decisions, its integrity — and the regular maintenance and commitment to its accuracy — is core to its intrinsic value.

Data must be precise to be useful in any productive way, and it must be accurate for the course of its lifecycle. It must be searchable, connected and recoverable. A company's decisions on its products, whether in the pharmaceutical field or not, can't be based on data that contains information gaps, report inconsistencies or undocumented sources.

A lack of adequate data integrity can cause multiple issues for companies. Information silos are often a result of poor data integrity, for example. When networks can't talk to each other, it drains company growth opportunities of their potential.

Unnecessary strain is put on business divisions forced into things like system workarounds to make sense of data that doesn't always mesh. Bad data can delay budget approvals and executive buy-in, hindering a company's agility and ability to be strategically nimble.

Data needs to be relevant and detailed in order for experts to analyze it accurately.

Though the methods of data integrity have changed and morphed over the years, they have been around for a long time.

**ALCOA and beyond**

The acronym ALCOA was first used by the Federal Drug Administration (FDA) in the 1990s to outline essential must-haves in data integrity. ALCOA stands for five facets of quality control. Whether on paper or digital, data must be **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal and **A**ccurate. The ALCOA system is a standard for data integrity.

Karl Fitt, Boston Analytical's Director of Quality Assurance, said that ALCOA is a start, but additional areas of data integrity should also include creating data that is Complete, Consistent Enduring and Available, known as ALCOA+.

For data to be **A**ttributable, one of the original ALCOA standards, he said, companies must ensure that work performed is electronically assigned to that person.

"There are other best practices, such as ensuring that work performed is electronically assigned to you," said Fitt, for example. "Don't piggyback onto other people's log-in credentials and log off after use. Companies can also set up software that can automatically log out a user or lock them out after a short period of inactivity."

Users verifying that they are officially logged on — checking the username on the display screen — is also a way to ensure data is attributable, said Fitt.

**Modern methods**

Maintaining Legible records, Fitt said, was something in the ALCOA system of standards that pertained more to paper recordkeeping. It was standard operating procedure to record data and sign off at the end of the workday, with no indication when exactly those activities took place throughout the day.

Digital systems are more seamless, he noted. But even with everything recorded digitally in today's day and age, legibility can refer to the fact that notations in electronic lab notebooks (ELNs) should be clear. Correct grammar and smooth flow that makes writing easy to follow now comprises this standard.

Keeping data **C**ontemporaneous means keeping it timely. Fitt recommends recording data in real time — not in segments and not all at the end of a report. "Electronic records now have a time and date stamp on every entry made, along with the username," he said, a tool to achieve better time transparency.

When it comes to data, it should be every company's goal to maintain the correct order of events, Fitt said. "This chronological flow is important. You can't transfer the balance weights after you've recorded the fact that you diluted or pipetted the resultant solution."

Ensuring data is **O**riginal translates into keeping original paper records, or if transforming into an electronic version of a record, verifying it as a true copy. Accurate records are complete, with nothing missing and truly reflect the activities detailed in that report.

The decades-old ALCOA standards eventually became ALCOA+, adding the importance of data also being **C**omplete, **C**onsistent (such as across system formats), **E**nduring and **A**vailable to those who need them.

Regarding Consistency in data integrity, Fitt uses printing chromatograms as an example of a situation that could compromise data integrity if not handled correctly. Chromatograms, visual depictions of the separation of a mixture, may show a need for change, he said. It's how that change is handled that impacts data integrity either adversely or positively.

"After it's printed, let's say you notice a small mistake in the peak identity," Fitt said. "So you annotate the paper by hand to correct. Now this is original GMP (Good Manufacturing Practice) data as well as the electronic original version. But now both versions do not state the same thing, so the original electronic version is no longer accurate," he said, adding that the electronic version should be annotated to show the same modification made to the printout.

But even with all ALCOA+ guidelines solidly in place, data accuracy is only as good as the users of that particular data network.

**User training, company culture**

How users interact with data software is, of course, the linchpin to data integrity across an organization. Even with high-level security policies in place and a corporate culture that is committed to best practices, data can be at risk.

"You can have some safeguards, but ultimately, you can't prevent humans from sharing things like usernames and passwords," said Fitt. But systems also must strike the right balance of security and functionality. Protections that are too prohibitive negatively impact those looking to access material for the right reasons, he noted.

"Sure, you could set up a system where each keystroke that each user entered required a password, but it would be too prohibitive, with work slowing to a crawl," he said. "There has to be some flexibility [with security] and training for employees. Companies have to strike that balance."

Businesses should ensure they put that balance in place, finding the right partners to make it happen, paving the way to company data integrity that is secure but accessible.



**"There has to be some flexibility [with security] and training for employees. Companies have to strike that balance."**

**-Karl Fitt,  
Director of Quality Assurance**

**Data delivery to start**

Delivering quality data that highlights accurate trends, gaps and customers is just the beginning.

Companies have to find ways to regularly ensure data integrity by performing audits that ask questions such as: Has it changed since the last review period? Is it accurate (or does it conflict with data stored elsewhere)? Is it readily retrievable?

The ability to assess gaps in data is another important part of the process. Data gaps represent areas that may be costing clients money, said Fitt. Pinpointing where these gaps exist is an important step toward deciphering what they mean.

Fitt is quick to point out that each client needs to access different data and each represents an individual relationship. There is no one-size-fits-all solution.

When it comes to data, some companies may prefer working with an expert partner that handles the number-crunching, relying chiefly on that partner's business guidance. Others prefer to be part of a more collaborative effort, offering crucial feedback and perspective.

Companies should seek out data partners that allow them the mode with which they are most comfortable, and know the value of data integrity. It is a true base for business growth.