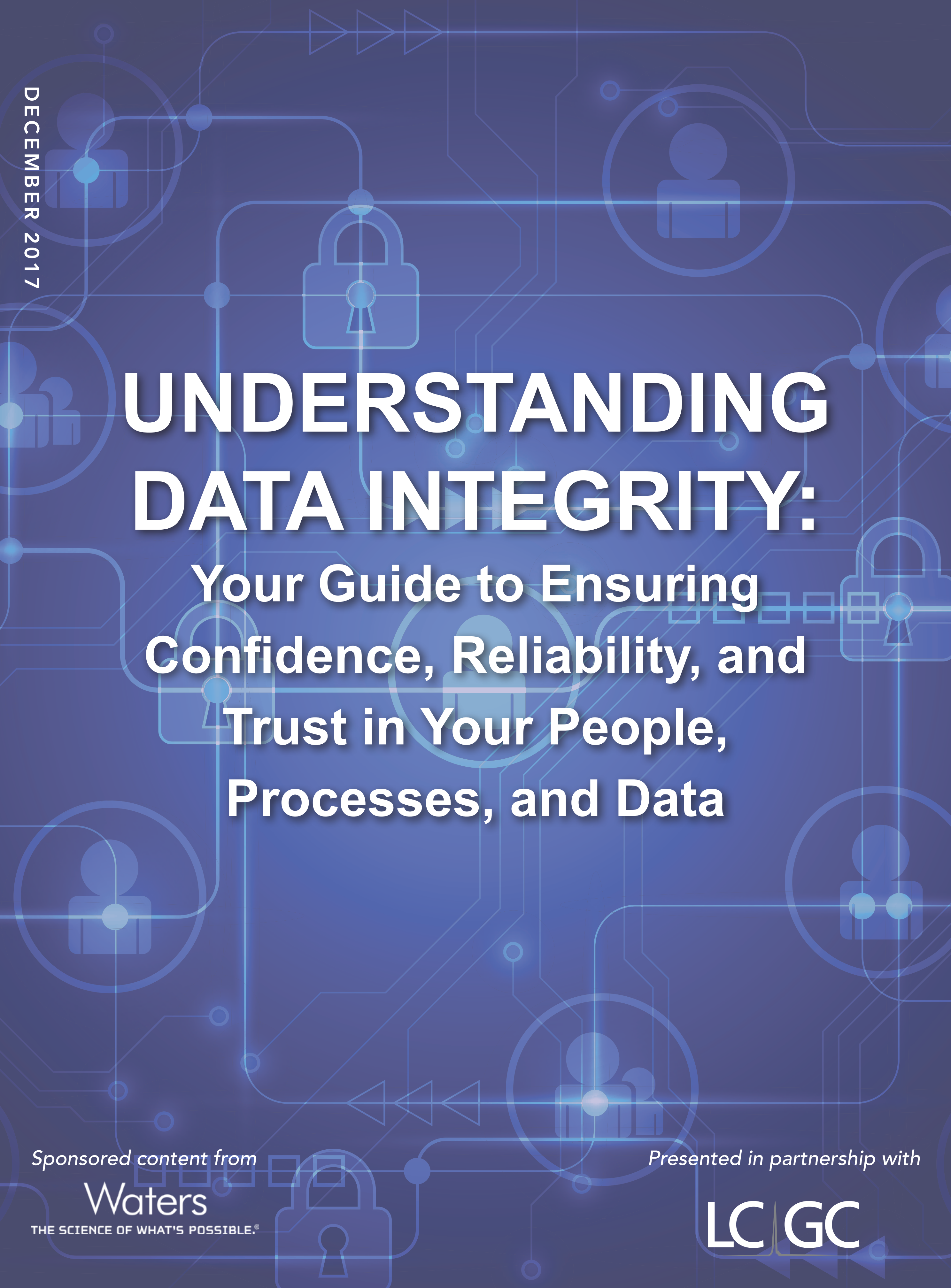
DECEMBER 2017



UNDERSTANDING DATA INTEGRITY:

Your Guide to Ensuring Confidence, Reliability, and Trust in Your People, Processes, and Data

Sponsored content from

Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

Presented in partnership with

LC GC

INTRODUCTION

Data integrity is a major concern for analysts in the pharmaceutical industry, as it is vital for ensuring product safety and quality as well as for maintaining regulatory compliance. As laboratories consider whether they are meeting regulatory requirements for their chromatgraphy data systems, they also must determine whether their validation efforts are on target, if there are holes in their risk management strategy, whether technicians fully understand their roles in maintaining data integrity, and much more.

For readers that want to learn more about these critical issues, this *LCGC* ebook dedicated to *Understanding Data Integrity: Your Guide to Ensuring Confidence, Reliability, and Trust in Your People, Processes, and Data* (with materials from our sponsor Waters Corporation) provides a rich collection of articles addressing several aspects of data integrity.

Heather Longden, the senior marketing manager for informatics regulatory compliance at Waters, kicks off the ebook with a discussion of the regulatory challenges of electronic data review including leveraging audit trails, cloud-based solutions, modernizing and automating analytical methods, and more. She discussess many obstacles that laboratories face in terms of electronic data management, and describes some options for addressing them. In a separate piece, Ms. Longden expands upon this discussion as she highlights solutions and challenges that surface in audit situations regarding chromatography systems.

Readers will also hear from Charlie Wakeham, a regional informatics Computerized Systems Validation (CSV) consultant at Waters, who explains how meaningful metrics collected as part of a data integrity plan can help senior management identify inefficiencies and improve their processes.

Rounding out the ebook is coverage of how automated archival solutions support long-term endurance of data in a similar manner to how automated backups ensure short term availability in the case of a data disaster. The final whitepaper explains how technical controls in CDS solutions can manage access to specific tools, or limit the data an analyst can view during integration and processing optimization.

While this book focuses on CDS systems, the principles and strategies outlined in the ebook can be leveraged to ensure data integrity across the scientific techniques in laboratories.

TOC

Table of contents

UNDERSTANDING DATA INTEGRITY:

Your Guide to Ensuring Confidence, Reliability, and Trust in Your People, Processes, and Data

This ebook is sponsored by Waters Corporation and is presented in partnership with *LCGC*.

New Challenges in Electronic Data Collection and Oversight

An Interview with Heather Longden

SPONSORED

Blog: Data Integrity Matters

Click to view blog

From better security and oversight, to improved flexibility and computing power, pharmaceutical companies are taking advantage of modern chromatographic techniques and electronic data solutions to keep ahead of data integrity challenges. In this interview with *LCGC*, Heather Longden, the senior marketing manager for informatics regulatory compliance at Waters, discusses the regulatory challenges of electronic data review including leveraging audit trails, cloud-based solutions, modernizing and automating analytical methods, and more.

LCGC: What are the biggest challenges to providing adequate oversight of electronic record-based processes?

Longden: In response to regulatory changes in the 1990s, pharmaceutical companies have been permitted to leverage electronic data to support laboratory tests, data-handling processes, equipment maintenance, and calibration records. Laboratories adapted to the idea of electronic recordkeeping, but few implemented systems with the understanding that the electronic data would need to be accessed and reviewed electronically to assure its quality.

SHUTTERSTOCK.COM/VOYAGER624

Many companies continue to rely on printouts, paper records, and written notes for review and oversight to some degree. This situation creates an opportunity for traceability gaps to develop. Paper records are only a snapshot or summary of the complete electronic data, therefore one cannot rely on paper records to confidently verify the accuracy of electronic records.

LCGC: How have companies responded to this oversight challenge in terms of their review process?

Longden: It depends on the complexity of the data. In an ideal situation, one would want everyone involved in regulatory audits (i.e., their customers, and their internal auditors as well as regulatory agencies) to examine the original electronic data on a regular basis. The complexity of understanding and interpreting that data requires a high skill level, which most closely aligns with the skills of those who work in the lab daily and the lab managers. Thus, the peer-review process takes on a much higher level of importance. In addition, QA groups are now much more involved in the design and validation of electronic systems and associated procedures. Consequently, the QA groups are still responsible for spot checking the electronic data (including all meta data) and ensuring the electronic review processes are being consistently followed.

This type of quality review and oversight level represents a shift away from a system in which QA teams attempted to look at every individual printed piece of data, to a new paradigm where they routinely check how the datasets being reviewed by the experts and how the systems and procedures are working.

LCGC: What are the consequences of discovering on your own, or having an outside agency discover, lapses in data integrity?

Longden: Companies are now expected to routinely review their data and procedures, and to proactively look for concerns about data integrity and opportunities for staff to manipulate data. If the lab determines that data integrity gaps could have affected information or products, the review process and impact assessment can be very costly and time consuming. Having to review historical data, potentially over several years, could include thousands of pieces of data. That vast analysis may require huge amounts of dollars and resources to investigate. One OTC pharmaceutical company reported a total cost of over $30 million to fully evaluate a potential data integrity breach, only to confirm that all the results they reviewed were fully correct and trustworthy.

If the gap was discovered by a regulatory agency, and be exposed as public knowledge, companies then have a major brand image problem to address in addition to the investigation costs.

LCGC: Why are some companies still relying on paper records at all?

Longden: Many quality groups are still insisting on being presented with data on paper so they can continue to leverage a pen signature to indicate review and approval. It allows a much simpler "compliance review" without expert knowledge of different computerized systems and the review process will be very uniform for all kinds of tests and across different vendor solutions.

However, health authorities such as the World Health Organization* clearly identify the risks associated with the limitations of reviewing only static and partial data that can be printed by laboratory and manufacturing software.

In today's laboratory, the original data in its electronic form is much more complete and retains its traceability in a far superior manner than can be achieved with paper reports. Reviewing the electronic records gives access to far more relevant information, ensuring greater confidence in the quality of the data.

Companies that are successful with the shift away from paper records find it beneficial to introduce a new data review approach. Peer review of the electronic data, documented with electronic signatures, is delegated to trained and trusted laboratory supervisors or experienced analysts.

In addition, some larger companies are dedicating certain individuals to new roles as data stewards. These individuals move away from regular laboratory analysis and data creation and instead are tasked with having an excellent understanding of the electronic data and becoming responsible for the quality of that data.

This contrasts with the traditional approach of the Quality Unit having eyes on every piece of data that's created. These Quality people now need the courage to devise a new risk-based approach to "how" and "how often" they oversee the data creation. This could include reviewing acknowledged summary reports and periodically ensuring that these contain the same data and results that can be found in the electronic data records. It is also important that a Quality Review process includes looking for undocumented or unreported data/results in the electronic data systems. This data, sometimes referred to as "orphan data," may be hiding unreported out-of-specification results or failing tests.

LCGC: What kinds of challenges are labs still facing in terms of electronic data management, and what technological solutions are available to help them?

Longden: More experienced companies only deploy networked, enterprise-level, integrated software solutions in the laboratory such as a chromatography data system or a company-wide LIMS. These solutions give individuals the opportunity to access data collected anywhere in their global network from any location. An impetus for this move has been the desire to have one single, secured data location, which also allows companies to conduct data review and oversight globally.

Less experienced laboratories still have a lot of standalone equipment. Without remote access to the data stored on these laboratory-based PCs, reviewing data electronically is a huge challenge. Recently, we've seen even small laboratories, which had previously preferred to deploy simple personal workstations, upgrade this equipment to enterprise systems because of their added security, automated back-up capabilities, and potentially better data oversight.

Another issue that can be addressed with enterprise systems is oversight of outsourced lab testing data. At the end of the day, the pharmaceutical company is responsible for the quality of the data collected by third-party partners and cannot solely rely on static, incomplete paper records. They must, therefore, have easy and continual access to the electronic records to be confident in the quality of outsourced activities.

It has been a challenge for companies to integrate electronic laboratory data from an outsource partner into a company's own data solutions to allow the expected level oversight of the CMO's or CRO's data.

Oversight across company boundaries is why many pharmaceutical companies are very interested in deploying Cloud-based applications. Cloud-based solutions help address complex quality oversight issues, allowing remote laboratories to be easily integrated into corporate CDS, ELN, LMS, or LIMS solutions. In response, Waters recently launched a new version of its compliance-ready chromatography data software called Empower Cloud. Working with Cloud partners Amazon Web Services (AWS), Empower Cloud has undergone documented testing as part of Waters Quality Management System to verify how deployment works through the Cloud and to ensure that the application continues to work reliably and robustly.

LCGC: Do you run into companies that still have concerns about the reliability and security of a Cloud-based system?

Longden: The security that the Cloud providers can offer is orders of magnitude stronger than anything that could have been provided by a third-party datacenter in the 1980s and 1990s. From a security and redundancy point of view, today's Cloud-based solutions are far more robust and many pharmaceutical companies are already using such solutions to support clinical trial data.

There are individuals who are concerned about Cloud-based solutions from a compliance point of view. Certain country regulations may indicate that data should be stored in the marketing organization's home country. Cloud vendors can certainly provide such assurances, if required.

Others are worried about the validation requirements when using a third-party Cloud provider for Cloud-based or -deployed solutions. The key to the validation project is to clearly understand the responsibilities of the Cloud provider versus the regulated company and leverage the expertise that Cloud providers can offer for redundancy, scalability, change monitoring capabilities, and security to support a regular validation project.

The regulators are writing into guidance documents that Cloud-based solutions are simply an alternative model of deploying computer hardware. If companies manage access, configuration, and apply change control as they would normally and have a good quality agreement that includes all parties' responsibilities (such as for backing up the data or documenting and validating changes), then regulators don't see anything special or different about Cloud-deployed systems.

LCGC: Let's shift to another key issue in data integrity. What is your view of the "bad actors" who appear to be attempting to pass off poor quality or poor studies as acceptable?

Longden: When I look at all the companies being cited or investigated for data integrity concerns, I believe there is only a very small proportion of truly "bad actors" who are deliberately flouting patient safety by falsifying and manipulating data. As a consumer, I am happy to see such unscrupulous companies being exposed and their products being removed from the supply chain.

Separately, some companies simply haven't made any effort to understand and implement good record management for both their paper and electronic records. For companies that really haven't thought at all about data integrity (and generally aren't meeting the minimum quality standards), Waters holds seminars about what we believe they should be taking care of regarding data integrity to minimize the opportunity for intentional or unintentional data manipulation.

A lot of people believe they've got everything taken care of (especially the technical controls), but there are areas where they are lax or they could do much more to ensure data is not manipulated, falsified, or altered in any way. In many cases, these improvements revolve around enhancements to the review process, to ensure that data is reviewed by people knowledgeable about the science and the data processing.

And then there's a large group of companies who really do have all their electronic systems controlled and managed, good quality processes, and knowledgeable staff members reviewing the data, but they sometimes find it difficult to express to an outside person how exactly they have data integrity under control.

Waters CDS solutions have been in use for maybe dozens of years in some companies. Sometimes, laboratories may be relying on old versions of the application, or maybe they have not had up-to-date training from the vendor for some time. As a vendor, we try to ensure these individuals have great documentation and training to help them clearly and confidently explain and demonstrate their understanding of their data systems.

LCGC: What are some common solutions for these clients?

Longden: Automate any part of the analytical testing process that can be automated, whether it's ensuring traceability across systems with automated data transfer or automating calculations that are currently done by hand. Each time human beings intervene in the process, there's a potential for mistakes, deliberate data manipulation, or the opportunity to "polish" failing results to ensure they pass specifications. Spending detailed time examining the human activity to ensure error-free work is generally a significant effort for quality assurance. Having the courage to critically review "the status quo" and invest in automation to remove data integrity gaps should result in a higher confidence in the quality of data generated.

A major root-cause for the need for human intervention in analytical testing is that many analytical methods used in today's marketplace, especially in the generics market, are *USP* (or other pharmacopeial) monographic methods or a company's own methods that have been in use for 15 years or more. Many of those methods are outdated, and could be redeveloped and improved to ensure more robust separation methods and right first-time automated peak integration.

However, companies often have a conservative approach to revising analytical methods. They feel they are validated and therefore shouldn't be changed. The reason for this belief stems from a variety of concerns: the effort and costs of revalidation and registration for new or changed methods with regulatory agencies, the worry about discovering new degradation products, impurities or other unknown peaks, or any other repercussions a change in the method may trigger.

Ideally, laboratory managers should be continuously looking critically at their analytical methods. The USP has initiated a program to update many monographs to include modern techniques. The more modern chromatographic methods would ideally be faster, but critically provide improved separation of components and higher resolution. This simple improvement should permit more robust analysis, and simpler automated integration for chromatographic methods, making it far easier to eliminate user intervention and be less challenging for laboratories to comply with data integrity requirements.

LCGC: Running an injection or two to be sure that a system is ready and fully equilibrated used to be a very common practice to ensure the quality of chromatographic data. Is this only

applicable for those older methods? Why do we hear that laboratories should no longer do test injections?

Longden: I've looked through all the different guidance documents from various agencies, and what you will read there is how to do test injections or, perhaps more correctly, systems readiness checks. The agencies never had any intention that people should stop doing test injections.

The guidances say that when you're doing those kinds of injections, you should use an independent sample or solution or a well-characterized secondary standard. The most important thing is that those systems shouldn't be a preview of the sample that you're about to analyze.

The issue that concerns the regulators is that when injections were found that were not included in the reported data, lab staff tried to pass them off as "test injections" when it was very clear that they were actual sample runs. It was simply an excuse for an "unofficial analysis" to be performed before they ran the official analysis.

The use of a system readiness test to evaluate the readiness of an LC or GC system is very much encouraged. This simple test should ensure that analytical results are not generated that must be scientifically invalidated due to a failure of the instrument or column. Why would the FDA guidance (for example) discuss how to perform such test injections if they were not allowed?

LCGC: What leads laboratory analysts to the need to reprocess data either using automatic or manual intervention?

Longden: If methods are robust, have great resolution for all peaks, and allow first-time integration automatically, then the need for reprocessing data can be nearly eliminated, except in cases where meta data was incorrectly entered. If this happens, the meta data needs to be amended and then the data reprocessed. Relying on older methods, and therefore on analysts' skills with the processing parameters to solve integration issues, is a major challenge today.

For some methods, a manual integration will be more accurate than any automated integration. Being able to understand when manual integration is justified and performed accurately, and reviewing the data with this perspective in mind, is why expert peer review is so important, especially in chromatography.

Laboratories that are struggling to meet arbitrary rules such as "No manual integration" or "No reprocessing without the permission of Quality person" will waste valuable resources to adjust and optimize integration parameters. The supervisors also lose transparency to the effort taken and therefore the ability to focus expert review processes on the most challenging separation results (i.e., those flagged as either manually integrated or that took several attempts to integrate accurately).

In my view, the most scrutiny should be on the results that only just meet specification, whether it's a high or low value. Only peak values that are borderline can be "polished" deliberately into specification by adjusting integration parameters, without it being graphically obvious in the integrated chromatogram.

LCGC: If a client purchased a software solution and it came with vendor qualification, do they still need to validate it?

Longden: While for extremely simple devices the answer is "probably", for chromatographic software the answer is simple; yes. Not all laboratories use a piece of software in the same way. While most labs will use a chromatography system similarly, the nuances of the system's use are really what you're trying to verify during the validation process.

So, to validate a computerized laboratory system of any kind, it should work in the way you expected, with your procedures, in the manner which you envisioned (i.e., fit for the intended purpose).

In addition, what you learn about a computerized system during the validation process is hugely valuable to your future use of it. Through validation, you might learn how to design different or better procedures, to be aware of any strange behaviors or abnormalities, or any nuances for how that software works compared to systems you may use already. And, your teams will be better able to articulate to an auditor or regulator how the system is configured and how it works within your laboratory SOPs.

LCGC: How important is retraining for your experienced clients?

Longden: Over the last 10 years or so, to keep up to date with new operating systems and, in the case of Waters, with new Oracle DB versions, new versions of laboratory software are continually launched and a client's QA and laboratory staff come and go. Yet, not all companies invest much in retraining on software they already use. They simply rely on their staff—new and old—to follow the same procedures without always fully understanding how everything fits together. When it comes to answering questions about how the systems were validated or how software applications work, the current staff may not know the answers over time.

The Waters technical field teams are strongly promoting the benefits of ensuring that the laboratory staff's knowledge of new software is up-to-date in the critical area of data integrity and that the software is more widely understood across the organization.

Our scientific experts are also well informed of the regulatory aspects of redeveloping, revalidating, and submitting enhancements to analytical methods for various agencies and can offer advice on this topic. This expertise provides the confidence and support for our customers who have the courage to make significant enhancements to their regulated laboratory work.

Heather Longden *is the Senior Marketing Manager of Informatics and Regulatory Compliance at Waters Corporation.*

Confidence, reliability, and trust in your people, processes, and data

Data Integrity refers to the overall completeness, accuracy, and consistency of data during its entire life cycle.

Though it seems simple, the whole process of genuinely generating, maintaining, and transforming data with completeness and accuracy is a challenging task for any organization. While today's focus may be seen to be software related, the underlying root causes of Data Integrity concerns step from poor management and culture, poor methods, poor separations, and poor education. Laboratories need to have confidence in the quality of their results and the methods they use to generate those results.

Partner with Waters

Through Waters' expertise in regulated environments and deep understanding of regulatory expectations, we are focused on working directly with your laboratory teams to provide the knowledge you need to manage increased regulatory pressures associated with the integrity and security of your valuable data.

Take a proactive approach to ensure the quality of your data. Identify and address potential issues before your next audit.

www.waters.com/dataintegrity

Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

Data Governance and Behavioral Controls

Charlie Wakeham

SPONSORED

Waters Explains Data Integrity

Click here to watch the video

Data governance is the total of all the activities and controls that are needed to ensure Data Integrity. The combination of these activities ensure that data, irrespective of the process, format or technology in which it is generated, recorded, processed, retained, retrieved and used will provide a complete, consistent and accurate record throughout the data lifecycle.

Data governance should not be seen as 'just another regulatory requirement'. When data governance is applied in a robust and effective manner, there will be business benefits in terms of minimizing product recalls and re-work, and reducing waste within the business process.

Meaningful and automatically-collected metrics around Data Integrity can provide senior management with the tools they need to identify inefficiencies within the organization and then focus their continual improvement efforts in that area.

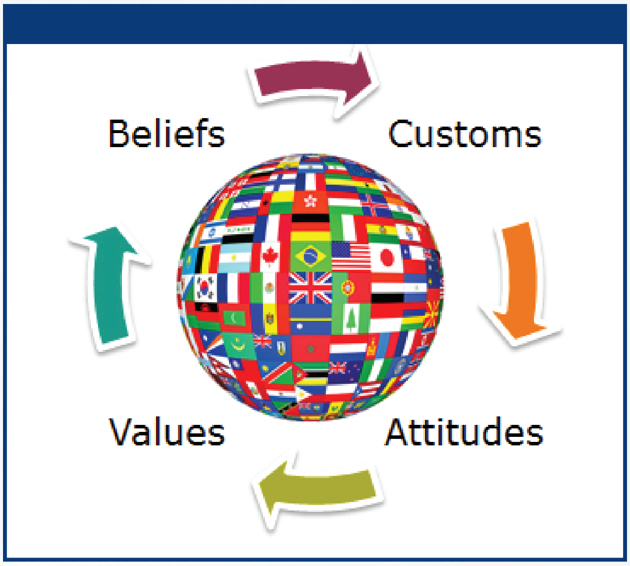
To achieve effective governance it is essential that senior management themselves set the example for appropriate behaviors. A management team which is heavily focussed on production yield and profits is never going to successfully create a corporate culture where Data Integrity and patient safety are protected at all costs.

In addition to the technical controls such as unique user accounts and audit trails which have been so widely discussed, data governance also includes the behavioral controls and quality culture which are needed for Data Integrity.

Culture is determined by a combination of beliefs, customs, attitudes and values created by the country in which a person was born and/or lives. This is then impacted by the corporate culture within a particular organization.

Open cultures have a more relaxed and informal management approach where any staff member feels comfortable to discuss problems and concerns either with their direct line manager or even with the next level manager. This is a very natural fit with the openness required for Data Integrity.

Closed cultures are often found in very traditional societies where the management style is highly formal and it is considered inappropriate or uncomfortable to give negative feedback or report a failure. Additional effort is needed to support Data Integrity within a closed culture. A confidential 'email hotline' is one effective option to give employees an anonymous way to reporting Data Integrity concerns without any fear of retaliation or negative consequences.



Regulatory guidances and warning letters have all shown that an audit deficiency can and will be given for the possibility of Data Integrity issues; for example, numerous warning letters cite analysts having delete privileges as a deficiency even if there has not been any deletion. The opportunity for deletion of data without any evidence of deletion occurring is enough to incur an audit finding. Similarly, if an auditor finds that an audit trail has been disabled that is seen as grounds for a critical deficiency—they don't need to find proof of any wrong doing in the period when the audit trail was inactive. When considering the intent behind a data integrity issue, the US FDA has clearly showed in at least one warning letter that lack of malicious intent does not in any way excuse a Data Integrity violation. This means that Data Integrity issues caused by genuine human error or lack of training are viewed just as seriously as deliberate data falsification.

Each and every person working with regulated data has the potential to protect or harm Data Integrity in some way, either within the permitted functionality of a computerized system or during a manual process for example by rearranging samples within an analysis sample set. A corporate Data Integrity training program is essential to provide knowledge and understanding of what Data Integrity is and why is it needed, and to promote awareness that a deficiency in Data Integrity at any point in the data lifecycle will impact all data downstream of that point, and ultimately resulting in patient harm.

Management focus should move away from automatically promoting and rewarding productivity and instead should focus on rewarding desired behaviours, such as the reporting of Data Integrity concerns and the open and honest discussion of failures or borderline results.

Data stewards are personnel with QA responsibilities who are given additional training to allow a deeper understanding of technical expectations and requirements, inspection and auditing techniques, and process controls. Data stewards may have a day to day role within the organization but also have an additional responsibility to 'stop the line' if they see any cause for concern around Data Integrity. Data stewards have immunity against any recriminations for their actions as guardians of Data Integrity.

The proof of an effective data governance program is if the regulated data meets all of the attributes of ALCOA+ such that it can be trusted for decisions relating to product quality, and that personnel have a detailed understanding of Data Integrity and its relationship and importance to patient safety. These elements need to be reviewed firstly at the system and department level, with all results then fed upwards to senior management (or a data governance council, if there is one). The results should then be used to determine the overall effectiveness of the data governance program, and the assessment of residual Data Integrity risk.

Charlie Wakeham *is a regional informatics CSV consultant at Waters.*

Why is Electronic CDS Data a Major Data Integrity Concern for Regulators?

Heather Longden

Tools and advice on electronic Data Integrity and how it specifically applies to chromatography systems and the challenges they present in audit situations.

Introduction

Pharmaceutical manufacturers are bound by regulatory agencies to follow and employ current Good Manufacturing Practices (cGMPs) for the preparation and analysis of drug products. Additionally, they have significant responsibility to demonstrate, document and file regulatory information before releasing new products to the market following Good Laboratory Practices (GLPs) and for proving clinical safety and efficacy following Good Clinical Practices (GCPs).

Analytical techniques, such as chromatography, are extensively used for measuring and quantifying components in a mixture, supporting many claims of product quality required by these GxPs. The chromatography data systems (CDS) used to capture, process and document the data have highlighted specific concerns about suspected regulatory and quality issues at some labs because the applications provided important benefits in terms of time-stamped, automated audit trails, change histories and

SHUTTERSTOCK.COM/PHOTOBANK GALLERY

(where used) secure electronic signatures. These technologies make data falsification more difficult and more traceable than with paper records; however, the added complexity and volume of available metadata presents its own challenges when devising comprehensive review processes.

What follows is a look at how chromatography data systems address specific concerns and challenges when demonstrating Data Integrity to an auditor or regulator.

Why Is Data Integrity of Particular Concern Today?

Data Integrity is not a new concern. It has been a regulatory expectation since written, and then printed, records were the norm. Today, however, the extent of metadata in electronic records is on a completely different scale; it provides significantly more evidence of a user's behavior than what would have been easily apparent in a written laboratory report.

Tools found in chromatography data systems should provide regulators additional confidence in the Data Integrity. However, as auditors and quality groups are learning how to read the metadata stored in electronic records, they are also highlighting potentially suspicious practices or those that cannot be readily explained. This is the source of today's strong focus on Data Integrity.

Unfortunately, agencies have lost trust that analysts always behave with honesty and integrity based on the additional information uncovered in the electronic records. They are now hoping that a lab's quality department will take advantage of this useful metadata to manage users' behavior and prevent falsified or even simply "polished" data. Regulatory agencies expect the quality unit and reviewers to monitor the data reported and to ensure that "testing into compliance" is not occurring.

What Is Data Integrity?

Data Integrity refers to the accuracy and consistency of data, facts and statistics over a product's lifecycle. Data Integrity ensures recoverability, searchability and traceability of any original records.

While software and built-in technical controls are key parts of Data Integrity, humans are the most critical variable because they create, review and approve the data. This can be seen significantly in chromatography versus other analytical or measurement techniques that are used to create data. Chromatographic analysis relies heavily on analysts' accurate adherence to procedures while preparing samples, standards and mobile phases and ensuring the instrument and chemistries are set up correctly before analysis, as well as scientifically evaluating and potentially reprocessing the data post acquisition, before the final results can be relied upon.

The human component relies on many aspects, including:

- A culture for Data Integrity
- Governance of data and quality focused review processes
- Data uniquely associated with specific users
- Users having the skill and the training to do the job in the most accurate way possible
- Safeguards against fraud

Analysts executing poor quality separation methods require additional manual steps to generate meaningful and consistent results. Therefore, to minimize the need for human intervention, laboratories should ensure the reliability and robustness of their separations. Analytical methods must be properly validated for accuracy, precision and robustness, while chromatographic instruments should be constantly evaluated for system suitability and robustness. Instruments must be regularly maintained as well as adequately qualified or calibrated throughout their use. Standards and reagents require accurate preparation in addition to high quality and reliable suppliers. Validated and documented procedures must be in place to minimize the potential for human error (malicious or unintentional).

Computerized Systems

At the request of regulators, Data Integrity controls are now expected to be built into chromatographic data collection applications and systems. Laboratory procedural controls should be in place for computer system validation, data traceability and periodic review of data handling. It is expected that software applications should only be run on a qualified network, should include a disaster recovery plan as well as backup and restore processes and all these aspects should be part of the validation process.

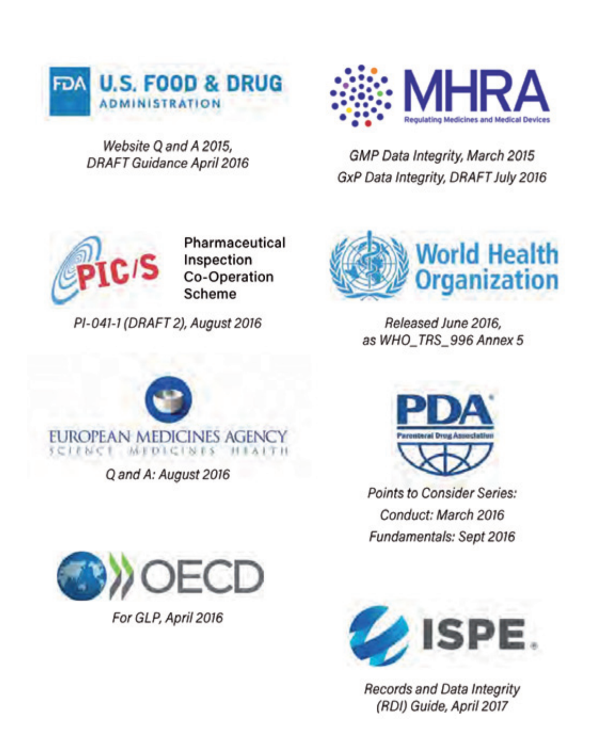
It is clear that computerized systems improve traceability and provide the capability to prevent and detect undesirable user actions by including more controls and documentation. Some basic tools for quality assurance (QA), quality auditors, and regulators include:

- Access levels
- System polices
- Audit Trails

Quality Data Review

Because of the tools offered by compliant-ready applications, it is critical that quality reviews, as well as inspections, focus on original electronic data in their original dynamic form. Related metadata, used to determine the trustworthiness of those data, are often missing from printed reports. This missing information may result in misleading interpretations leading to quality risks. Regulators are also hiring investigators or auditors with laboratory backgrounds who understand the systems, and some are learning how a good well-controlled laboratory should function, from the laboratories that they visit.

Presenting both the good as well as the "less-than-perfect data" is necessary to demonstrate that errors are not ignored or dismissed, specifically for reanalysis and reprocessing. A proper process must be followed for a lab error investigation to determine if the root cause could be assigned to a mistake in the analysis. Only then can repeat testing be performed. If no lab error is clearly identified, a full out-of-specification (OOS) investigation should be initiated to determine the cause of a product quality failure.


FDA U.S. FOOD & DRUG ADMINISTRATION
MHRA Regulating Medicines and Medical Devices
PIC/S Pharmaceutical Inspection Co-Operation Scheme
World Health Organization
EUROPEAN MEDICINES AGENCY SCIENCE MEDICINES HEALTH
PDA Parenteral Drug Association
OECD
ISPE

Website Q and A 2015,
DRAFT Guidance April 2016

GMP Data Integrity, March 2015
GxP Data Integrity, DRAFT July 2016

PI-041-1 (DRAFT 2), August 2016

Released June 2016,
as WHO_TRS_996 Annex 5

Q and A: August 2016

Points to Consider Series:
Conduct: March 2016
Fundamentals: Sept 2016

For GLP, April 2016

Records and Data Integrity
(RDI) Guide, April 2017

Figure 1: Data integrity guidances.

Guidance Documents

Regulators need to trust the data they are presented with as this is what they rely on most to ensure the quality of work performed when they are not in the laboratory. As a result, many guidances have been written about Data Integrity and, although written by several different agencies and industry groups, they are well aligned (**Figure 1**).

Both final and draft guidance documents indicate that data must be ALCOA:

- **A**ttributable to a particular user
- **L**egible (clear and concise data entries)
- **C**ontemporaneous (recorded at the time of the activity)
- **O**riginal (i.e., the first recorded observation or a verified true copy of the original observation)
- **A**ccurate (scientifically valid and error-free)

In addition, data must be (+):

- complete (including any repeat processing)
- consistent
- enduring
- available

The challenge for chromatographic analysis is its complexity. As instrumentation becomes more sophisticated, printouts only summarize the data (in static form) and are not a complete representation of the original (dynamic) electronic record. Printed chromatograms do not satisfy the GMP requirements that any printed record should be a true, accurate and complete copy of every item stored as part of the electronic record.[1]

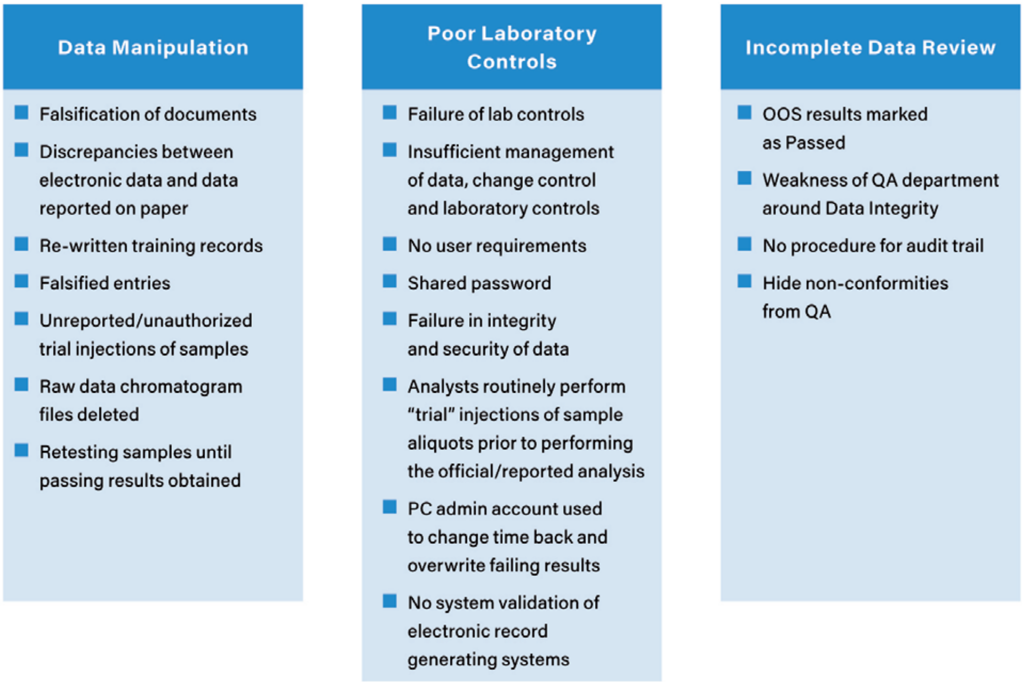
Regulatory Concerns for Data Integrity

Failure to establish that lab records include complete data is a GMP violation of 211.194(a). Firms must keep all data associated with an analysis and all calculations performed whether they were correct or incorrect and whether they needed to be repeated or invalidated.

European Union (EU) non-conformance reports include observations of a) manipulation of laboratory data, b) the opportunity to manipulate data based on missing technical controls, and c) incomplete data review processes, which should be able to intercept manipulated data (**Figure 2**).

Regulators are often starting from the assumption that data is not being captured and reported with honesty and integrity. It then becomes the job of the laboratory to prove otherwise. Key inspection themes are outlined in **Figure 3**.

One way to prove integrity is through technical controls. If systems do not allow users to delete data, it becomes easier to prove that data could not have been erased. Shared accounts are also problematic for demonstrating unquestionable accountability for data creation or modification. Many laboratories are still



Data Manipulation

- Falsification of documents
- Discrepancies between electronic data and data reported on paper
- Re-written training records
- Falsified entries
- Unreported/unauthorized trial injections of samples
- Raw data chromatogram files deleted
- Retesting samples until passing results obtained

Poor Laboratory Controls

- Failure of lab controls
- Insufficient management of data, change control and laboratory controls
- No user requirements
- Shared password
- Failure in integrity and security of data
- Analysts routinely perform "trial" injections of sample aliquots prior to performing the official/reported analysis
- PC admin account used to change time back and overwrite failing results
- No system validation of electronic record generating systems

Incomplete Data Review

- OOS results marked as Passed
- Weakness of QA department around Data Integrity
- No procedure for audit trail
- Hide non-conformities from QA

Figure 2: Summary of EU non conformances.

using instrumentation with software that has no audit trails, which is a failure to meet the technical controls requirements set out in 1997.

Additionally, managers should be sure that simply hiding or ignoring data is not occurring, specifically when a run must be repeated. This might include a defined investigative process and proper scientific justification for invalidation of any data. FDA and other agencies provide detailed guidances on these expectations.

To ensure drug quality, regulatory agencies will look at and expect in-house quality units to continuously observe all reported and non-reported electronic data (orphan data):

- Are analysts cherry picking only the good results?
- Are samples being "tested into compliance" or polished to meet specification?
- Is data secure?
- Is there hidden or deleted data?

This problem is tied to OOS results, which may be either ignored or invalidated without proper justification and then simply retested. In these cases, the data review often does not include the original and all versions of results. Moreover, orphan data captured to a "test" folder without proper scientific invalidation could cause suspicion as deliberately cherry picking or making the results look better.

Properly looking for the root causes of invalidated results, whether for "in specification" or OOS results, and eliminating

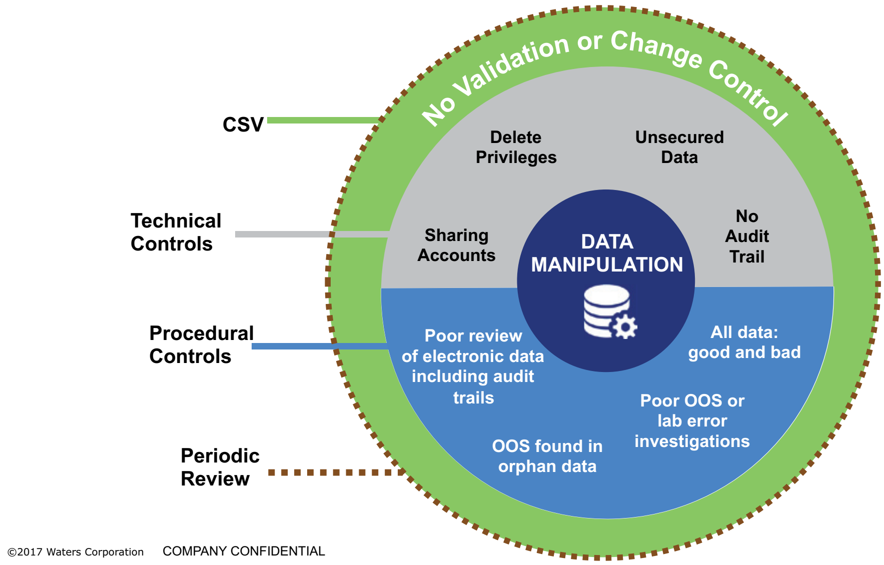


Figure 3: Inspection themes.

that root cause problem, will subsequently reduce the need for any future repeat testing. Root causes that can be addressed to prevent future failures and reprocessing include:

- Poorly developed or validated analytical methods
- Inconsistent column separation performance
- Sample, standard, reagent or mobile phase preparation errors
- Instrument failures
- Analyst error

Specific Concerns about the Chromatographic Process: Repeat Injections and Test Injections

Guidances suggest that reanalyzing or reintegrating a sample should never be required; however, tests fail for a variety of reasons such as instrument failure, lack of system equilibration, improper/expired columns, or a mistake. When a mistake is made, there is often pressure to rectify or hide the problem.

Justifications such as "I'll be fired if I admit my mistakes," "I have no time to do an OOS investigation," and "No one will notice if I'm clever about covering it up" are probably the biggest reasons why analysts attempt to hide errors in their lab from their own quality units.

It warrants repeating that there must be a scientific reason for reanalyzing samples. This should be documented in a deviation report (or similar document) and regulators are concerned if only the repeat sample set is reported. If the data is documented as a repeat, regulators/auditors want to see the original data and the scientific justification for the repeat.

Test injections may be viewed with concern if they routinely use sample preparations to ensure systems are ready for use. While it is scientifically sound that no analysis should be initiated until chromatographic systems are functioning properly, test injections from samples should not be used for this purpose. This could potentially raise a regulatory issue and suspicion of pretesting or unofficial testing of the sample. Also, analysts sometimes try to justify a failed series of injections as simply a test of the system. An independent solution or a well-characterized secondary standard, for instance, is a better choice for test injections or "system readiness checks."

If system suitability is not met, ideally the run should be aborted to ensure questionable data is not produced or collected. Alternatively, it may be sufficient to ensure that any data collected is not processed if it could not be trusted due to a system suitability failure. One way to minimize the occurrence of failing chromatographic systems is to ensure that both equipment and methods exceed robustness expectations. This would reduce analytical runs that need to be repeated.

Specific Concerns about the Chromatographic Process: Reintegration of Chromatograms

Documentation of why an analyst reprocesses chromatograms should be available. This might be simply recorded in the comments that form part of the required audit trail, or it may need additional documentation. However, reviewers and QA must appreciate that it is unrealistic to expect chromatography to integrate perfectly the first time every time. Unless the laboratory has very clean, robust and well resolved chromatograms, it is perfectly normal to require some optimization of integration or identification parameters for each day's run. If a laboratory gets perfect integration right the first time for all chromatograms, it may raise suspicion. If the data looks too good to be true, then it probably is.

Multiple integration attempts could indicate deliberate polishing or manipulation or at least give rise to questions, specifically if the sample or run failed in the original integration and passed when reintegrated.

Reviewing audit trails and original processed data is the only way to determine if reprocessing was scientifically required or conducted for another reason.

Automated processing (i.e., leveraging the algorithms and integration parameters in the processing method) is only an approximation of the peak integration that a good chromatographer would manually assign, leveraging their own scientific knowledge and experience. Preference may be to use software for convenience and speed of processing results with some idea it creates consistency. However, automation does not bestow a higher level of quality on the integration.

Processing parameters must often be adapted by analysts to get the most accurate peak integration, especially if the run includes very disparate levels of component concentrations. A single accurate set of parameters to automatically process the entire data set sometimes cannot easily be derived. In such cases, manual integration may be required for individual runs to ensure accurate integration.

The alternative practice of optimizing integration parameters to a new version of method, for each and every sample, is rarely viewed as good practice. Confidence that calibration standards, system suitability chromatograms and sample analyses are all processed using the same set of processing parameters is expected. Some CDS applications, such as Empower, will rely on the assumption that standards and samples will be processed using the same version of the processing method.

Saving each version of results is a key element that the FDA guidance includes. Each reprocessing or reintegration is part of the GxP record, and should be reviewed to ensure that subsequent iterations were not processed to polish or hide OOS results. It may also be possible in the CDS to obscure from the analyst the effects of integration changes to calculated values so as not to influence the placement of baselines, either automatically or manually.

Forcing lab processes that only allow automated processing of chromatograms will result in staff spending large portions of their day programming integration events to ensure that the resulting peaks are integrated correctly, with no obvious indication of manual intervention. Complex parameters and timed events in an automated integration process can ultimately be equivalent to manual integration (such as the "forced peak start" event). The degree of manipulation that can be done under the auspices of an "automated method" might be as customized as a manual integration activity could produce. In this case, the degree of human intervention is of a similar level, and yet the casual reviewer will not easily see how manipulative the analyst has been. Clearly and transparently using manual integration may well result in higher level of quality.

The placing of baselines, specifically for unresolved peaks, should always follow expectations consistent with the method as it was validated. Each day's analysis will not be identical to the previous day. Therefore, a clear procedure for adapting the integration to the raw data should be expected with appropriate levels of oversight.

A quality method with good resolution enables the analyst to have a processing method that performs integration reproducibly the first time. Training on how to use the integration parameters is essential as well as having wellunderstood

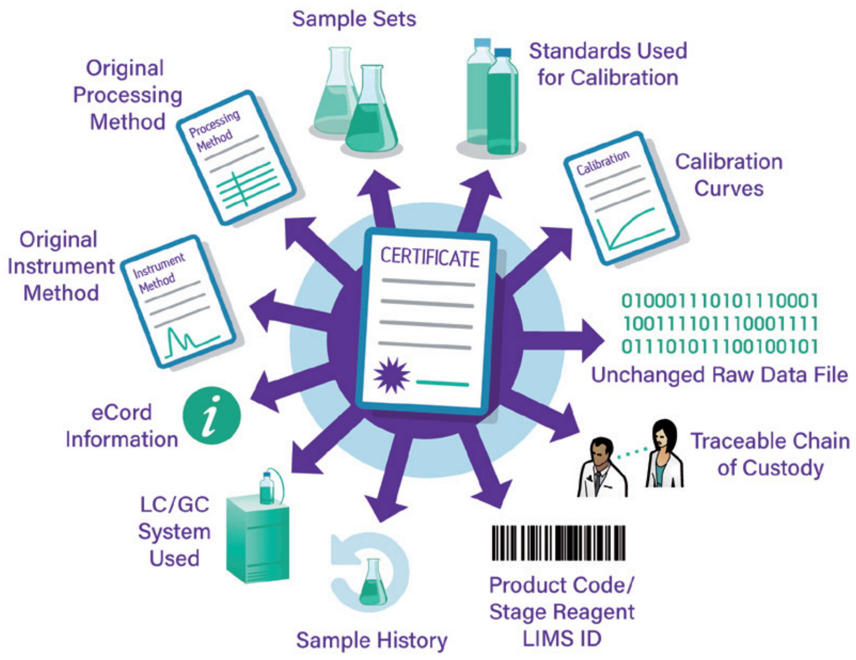


Figure 4: Traceability through Empower®.

procedures for processing and reprocessing chromatograms including good examples of the expected integration for each individual method (product or analyte specific). Reviewers should pay special attention to data that is reprocessed, whether with automated algorithms, with highly customized integration events, or manually.

Traceability

Audit trails should be included in the electronic meta data and be an integral part of the review process. It provides history and supports trust for the results being reviewed. The level of review and oversight that audit trails provide also deters analysts from using shortcuts in the system or manipulating the data.

Current chromatography data systems offer an internal database, which is an important traceability tool. Chromatography systems equipped with Waters® Empower® Software can link all aspects of metadata together into a traceable solution to ensure that metadata links can never be broken (**Figure 4**).

Summary

Chromatography data systems capture important information (or metadata) for electronic records including audit trails which leverage time stamps and change histories. To ensure product quality, the metadata should be regularly reviewed by quality control staff to manage users' behavior to prevent generation of falsified data – either maliciously or inadvertently.

Establishing a culture where laboratory staff are empowered to raise and act upon concerns about product quality issues, analytical method improvements or workflow enhancements is essential. Equally, imposing unreasonable barriers to analytical work, in an automatic, immediate reaction to regulatory observations, might simply tempt staff to find alternative ways to achieve their work goals. Companies need to balance critical compliance measures against the practicality of the implementation and the needs of the business to ensure consistent quality of analytical results.

Reference

(1) FDA, "Data Integrity and Compliance With CGMP Guidance for Industry," April 2016, https://www.fda.gov/downloads/drugs/guidances/ucm495891.pdf

Heather Longden *is the Senior Marketing Manager of Informatics and Regulatory Compliance at Waters Corporation*

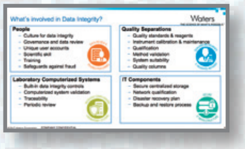
System Policies and Privileges for Processing Data in Empower Software with Data Integrity in Mind

Neil Lander

SPONSORED

Click to watch the webcast

Balancing Technical Controls, Tools, Transparency, and Trust for a Culture of Data Integrity



What's involved in Data Integrity?

Waters

People
- Culture for data integrity
- Governance and data review
- Unique user accounts
- Scientific skill
- Training
- Safeguards against fraud

Quality Separations
- Quality standards & reagents
- Instrument calibration & maintenance
- Qualification
- Method validation
- System suitability
- Quality columns

Laboratory Computerized Systems
- Built-in data integrity controls
- Computerized system validation
- Traceability
- Periodic review

IT Components
- Secure centralized storage
- Network qualification
- Disaster recovery plan
- Backup and restore process

Explore how Empower® Software System Policies and privileges can be used to control what users can or cannot do when processing data, particularly when working in the Review window

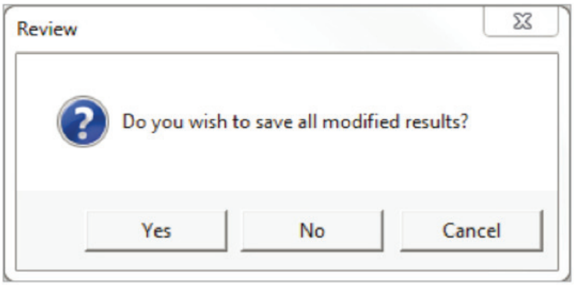
Introduction

With increased scrutiny around Data Integrity, it is important for Quality Units and Regulators to understand the Empower® Software capabilities for processing data and the need for varied levels of flexibility. There is a perception that analysts may 'polish results' and cause otherwise out of specification (OOS) samples to pass laboratory test requirements, such as assays and impurity methods. In order to fully ascertain what is happening in the laboratory, both the Quality Unit and Regulators should be fully aware of how an organization utilizes the Review window to optimize Processing Method parameters. This white paper will walk through the current System Policies and privileges in Empower 3 that effect what analysts can and cannot do when processing data, focusing on the use of Review.

System Policies

System Policies control the behavior of Empower Software for the whole application.

SHUTTERSTOCK.COM/MAKSIM KABAKOU



Review

Do you wish to save all modified results?

Figure 1: Save results message when exiting from Review.

They also control certain aspects of how all users accessing the system interact with the software. The Empower system administrator can set rules governing user accounts, log in procedures, full audit trail default settings, data processing techniques, result sign-off requirements, and date formats. System Policies help define the peak detection and integration techniques, and calculations that Empower uses to process data.

There are several general data processing System Policies which effect processing data:

- **Calculate % Deviation of Point from Curve** – changes the formula for calculating % deviation.
- **Allow Interactive System Suitability when acquiring in RUN ONLY mode** – Interactive System Suitability, such as Stop on Fault, can be triggered when in Run Only mode. It is recommended to operate in the Run and Process mode so that all result(s) will be saved in a regulated environment.

There are also System Policies which control the use of the Apex Track Algorithm:

- **Allow the use of Apex Track Integration** – Enables the use of the Apex Track algorithm in the Empower database.
- **Default settings used when creating new projects.**
  - — Enable Apex Track Integration: Sets the default for new projects.
  - — Default Integration Algorithm: Sets the default for new Processing Methods.

There is also one critical policy which adds a control for users working in Review:

- **Prompt user to save manual changes made in Review** – If a user exits from Review after creating a result(s) they will be prompted to save the result(s). In **Figure 1** the message reads, “Do you wish to save all modified results?” If users save results at this point, it will automatically save the last version of all results and any related changes (i.e. calibration curves or methods).

Any results saved in the Review window in this manner will automatically be labeled as manual results regardless of whether manual integration was used.

Processing Method Privilege Options

Empower Software allows users to operate under a set of defined privileges that collectively define an overall user type. It is possible for an individual user to be able to log in with a different user

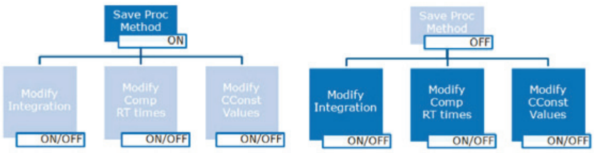


Figure 2: Hierarchy of Processing Method privileges. The bold color indicates which privileges are in effect.

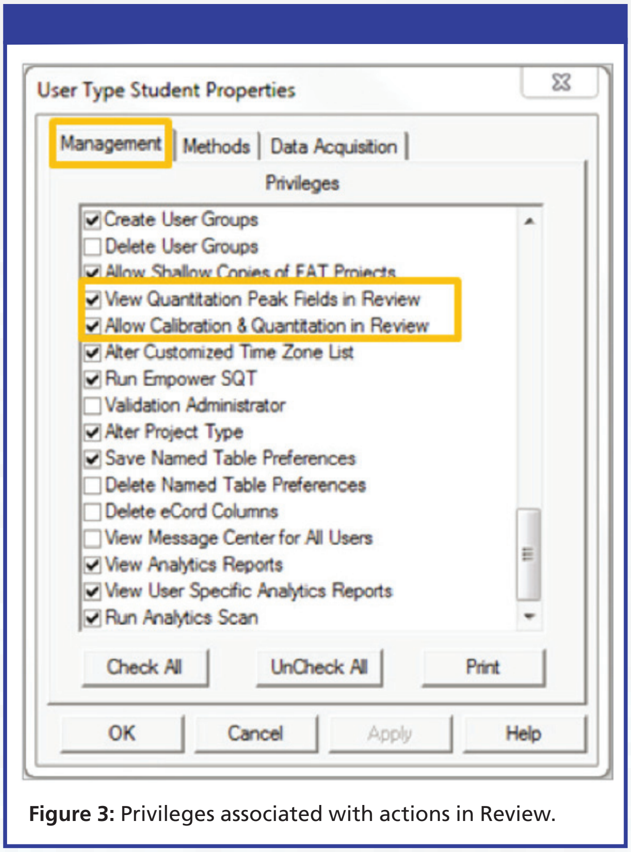
type, with a different set of privileges, if they have to perform a specific task. Depending on the tasks performed, the system administrator can assign or remove the privileges associated with a user type. In order to properly validate Empower it is extremely useful to understand how these privileges operate and to document the privileges that laboratory users need to perform their work.

The privileges associated with processing methods have a significant effect on what users can do in the Review window:

- Lock Methods – A locked method can be used to generate results, however, it cannot be modified. Locking a method is a permanent action and cannot be undone in Empower 3 FR4 and earlier versions.
- Delete Processing Methods – This privilege should only be granted to a high level administrator. It should be noted that any processing methods associated with existing results will not be deleted.
- Save Processing Method – Allows the user to create new processing methods and/or modify existing processing methods. This allows users to modify ALL parameters in any section of the processing method. It is important to note that the more detailed privileges described below have no effect if this privilege is granted (**Figure 2**).

If the Save Processing Method privilege is NOT granted, the ability to modify a processing method depends on whether or not any of the next three privileges are granted. This enables an administrator to grant access to only specific parameters in the processing method.

- Modify Integration Parameters – Allows the user to modify peak detection and integration parameters on the Integration tab, such as peak width and detection threshold. This privilege is required for users to optimize integration and account for day-to-day variation in peak shape.
- Modify Component Times – Allows the user to modify the expected retention times of named peaks on the Components tab. This privilege is required for users to account for day-to-day variation in retention times and ensure correct peak identification.
- Modify Component Constants/ Default Amounts – Allows the user to modify the CConst fields on the Components tab. This may be required to modify constants used to capture values such as Label Claim or Moisture Content, when these values periodically require updating. It is important to note that in the current



- ☑ Create User Groups
- ☐ Delete User Groups
- ☑ Allow Shallow Copies of FAT Projects
- ☑ View Quantitation Peak Fields in Review
- ☑ Allow Calibration & Quantitation in Review
- ☑ Alter Customized Time Zone List
- ☑ Run Empower SQT
- ☐ Validation Administrator
- ☑ Alter Project Type
- ☑ Save Named Table Preferences
- ☐ Delete Named Table Preferences
- ☐ Delete eCord Columns
- ☐ View Message Center for All Users
- ☑ View Analytics Reports
- ☑ View User Specific Analytics Reports
- ☑ Run Analytics Scan

Figure 3: Privileges associated with actions in Review.

version of Empower, users will not be able to modify Default Amounts even with this privilege enabled.

There are instances, when working with Impurity methods for example, where it becomes necessary to modify integration parameters and component times due to complex chromatography. Collectively these privileges allow a company to tailor a user's ability to modify specific parts of the processing method.

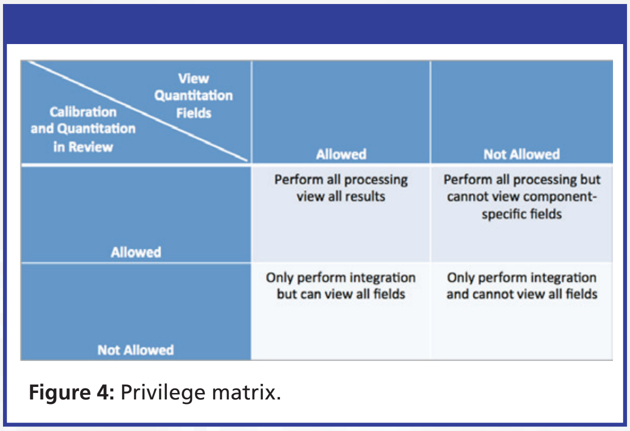
Review Window Privilege Options

The privileges associated with calibration and quantitation have a significant effect on how far through the workflow of processing data and generating results is possible in Review. These are also used to limit the calculated peak values viewable in Review prior to data processing.

- View Quantitation Peak Fields in Review – Allows the user to view the following fields in the Review window peaks table: Area, % Area, Height, % Height, Amount, % Amount, Response, and Concentration. Users not assigned this privilege cannot view these fields nor will they be visible in the properties of the peak table.
- Allow Calibration and Quantitation in Review – Allows the user to calibrate and quantitate data in the Review window. Users not assigned this Privilege cannot calibrate and quantitate data in Review. They cannot add, insert, delete or modify points on the calibration curve, individual-point table, or delete points on the calibration curve plot. Disallowing this privilege removes the ability of a user to see peak/component identification or any component-specific processing values in the peaks table or plot for any unsaved live data they are working with in Review (**Figure 3**).

There are several possible scenarios resulting from an analyst being assigned these privileges for working in Review. Here are some examples (**Figure 4**):

- Analyst has the Allow Calibration & Quantitation in Review privilege but not the View Quantitation Peak Fields in Review privilege.
  - — The analyst can use the Integrate, Calibrate, and Quantitate tools.



Calibration and Quantitation in Review \ View Quantitation Fields	Allowed	Not Allowed
Allowed	Perform all processing view all results	Perform all processing but cannot view component-specific fields
Not Allowed	Only perform integration but can view all fields	Only perform integration and cannot view all fields

Figure 4: Privilege matrix.

- — The analyst cannot see the Area and Amount fields.
- — However, limits set in System Suitability will be effective and will indicate pass/fail. And, any component specific tailored calculations will be calculated and displayed.

- Analyst has the View Quantitation Peak Fields in Review privilege but not the Allow Calibration & Quantitation in Review privilege.
  - — The analyst can use the Integrate tool but not Calibrate or Quantitate tools.
  - — The analyst will see Area and %Area.
  - — Amounts and other component specific fields are not generated.
  - — The analyst will not be able to view and determine pass/fail on System Suitability limits nor calculate or view component specific tailored calculations.
- Analyst does not have Allow Calibration & Quantitation in Review or View Quantitation Fields in Review privileges.
  - — The analyst will only have the ability to optimize the integration graphically.
  - — The numbers of text and numerical values which can be viewed are severely restricted.

Purposeful management of these two privileges can allow an analyst to optimize a Processing Method in the Review window, with a view to using that method to batch process results, but limit the information they can create or view while performing that optimization.

Saving Results Privilege Options

Typically processing of samples to create results will be performed using batch processing. This ensures consistency and is much more efficient than processing through the Review window. Batch processing is required to achieve more sophisticated quantitation practices such as bracketing, summary custom fields, or using multiple processing methods for defined samples in the Sample Set.

The privileges associated with saving results can have a limiting effect on what analysts can do in Review:

- **Save Results** – Allows the analyst to batch process as well as save results while working in Review. Analysts not assigned this privilege cannot save results in any part of Empower.
- **Save Results and Calibrations in Review** – This allows the analyst to save results while working in Review.

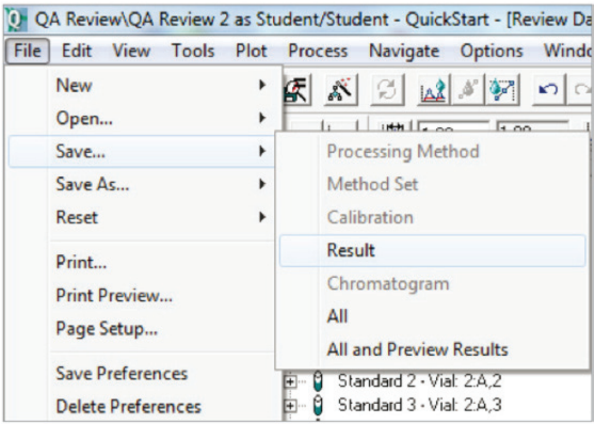


Figure 5: Manually saving results in Review.

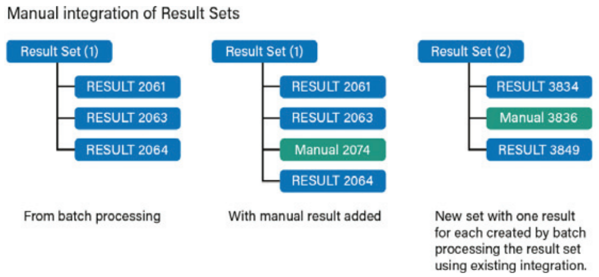


Figure 6: Saving a manual result into a Result Set and batch reprocessing a Result Set containing manually integrated chromatograms, with Use Existing Integration

Analysts not assigned this privilege can batch process; however, they cannot save any results while in the Review window.

Saving Manual Results in Results Sets

If data requires manual peak identification or manual integration, analysts may need to process and save results in Review. After bringing a Result Set into Review, analysts may perform manual integration and quantitate samples. Saving this result will add it to the Result Set. It is important to note that this does not apply when standards are calibrated in Review.

This privilege is required if a company perceives a need to Save All results created in Review and leverage the system policy described at the beginning of this white paper.

An alternative control might be to have analysts save only manual integration in the Review window (see **Figure 5**). This allows manual integration of both samples and standards. Analysts could then batch process with the Use Existing Integration feature to quantitate a Result Set that retains the manually integrated peaks for both samples and standards (see **Figure 6**).

Knowing how these privileges impact processing of chromatographic data in the Review window helps laboratory supervisors better understand how data is generated by analysts. Concerns exist about an analyst's ability to fine tune the integration of peaks in a sample to bring failing results into specification. However, this would only be possible for samples which are very close to specification without creating obviously 'incorrect' integration.

For example, viewing a set of data as shown in an Empower control chart (**Figure 7**), the five results closest to the lower control limit may have been integrated into a passing state.

Control charts are easily generated within Empower reports and provide laboratory supervisors a visual tool to look for trends in results.

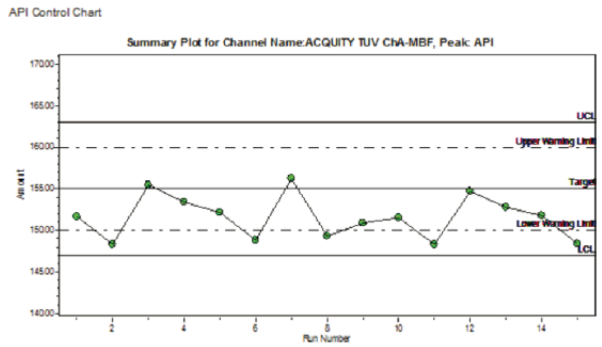


Figure 7: Control chart illustrating batch results exceeding warning limits yet passing specification.

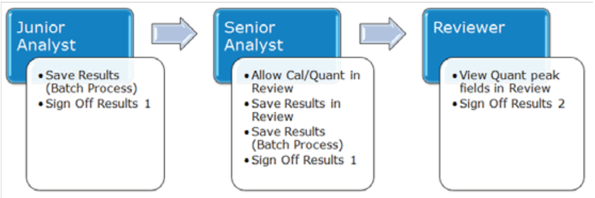

Junior Analyst
•Save Results (Batch Process)
•Sign Off Results 1
Senior Analyst
•Allow Cal/Quant in Review
•Save Results in Review
•Save Results (Batch Process)
•Sign Off Results 1
Reviewer
•View Quant peak fields in Review
•Sign Off Results 2

Figure 8: Example of tailored User Types.

Combining Privileges to Manage How Users Interact with Data in Review

Figure 8 is an example of how privileges might be assigned depending on job function within an organization.

Remember that a user who normally logs in as a Senior Analyst, may need to switch roles by logging out and logging in again in a Review role.

Additional Considerations for Data Integrity

Locking Channels from further processing

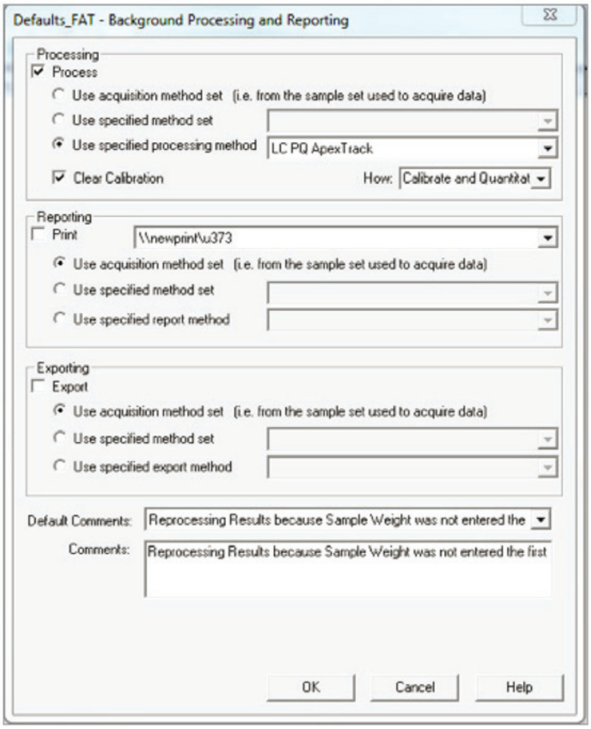
There are two further privileges associated with locking channels: Lock Channels and Unlock Channels.

Once results have been generated the associated channels can be locked so that users cannot generate any further results. In a Quality Control (QC) laboratory it is common for a channel to be locked once the result has been signed off. If a result is deemed inaccurate the channel can be unlocked for further processing by a user with the privilege to do so.

- A user can view the information associated with a locked channel.
- Allow Lock Channels after Sign-off 2 is a system policy that, when enabled, would allow a channel to be locked after Sign-off 2 in the Sign-off dialogue box.

Recording the reason "why?" for saving results

- Empower automatically records what actions were performed in the various audit trails and the user needs to document why they were performed.
- Users are typically expected to enter reasons why changes were made to project level objects such as methods, and system level objects such as chromatographic systems. It is important that these reasons reflect 'why' changes were made rather than 'what' changes were made. In regulated laboratories this is likely to be a requirement. In non-regulated laboratories it is not a requirement; however, these reasons add value by giving extra details about activity in



Defaults_FAT - Background Processing and Reporting

Processing

☑ Process

○ Use acquisition method set (i.e. from the sample set used to acquire data)

○ Use specified method set

● Use specified processing method: LC PQ ApexTrack

☑ Clear Calibration — How: Calibrate and Quantitat

Reporting

□ Print: \\newprint\u373

● Use acquisition method set (i.e. from the sample set used to acquire data)

○ Use specified method set

○ Use specified report method

Exporting

□ Export

● Use acquisition method set (i.e. from the sample set used to acquire data)

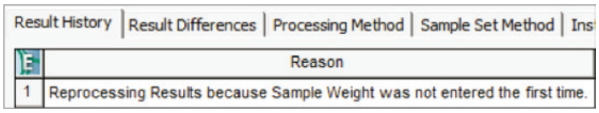
○ Use specified method set

○ Use specified export method

Default Comments: Reprocessing Results because Sample Weight was not entered the

Comments: Reprocessing Results because Sample Weight was not entered the first

Figure 9: Background Processing and Reporting dialogue box showing the reason 'why' in the Comments box.



	Reason
1	Reprocessing Results because Sample Weight was not entered the first time.

Figure 10: Reason why a result was reprocessed in the Result Audit Viewer.

Empower and could be seen as good practice.

- For example, when an analyst processes a Sample Set, the selection of the reason why is done in the Background Processing and Reporting dialogue box (**Figure 9**).

The reason why a Sample Set was processed would then appear in the Project Audit Trail and the Result Audit Viewer (**Figure 10**).

There are two approaches to entering these comments – in an unrestricted manner or a restricted manner. Unrestricted allows the user to enter the reason why as free text. Restricted entry requires the user to select a predefined reason from a list. These predefined reasons are called Default Strings. It is important to make sure the Default Strings reflect the reason why an action was performed. Default Strings are created in Configuration Manager and can be created by any senior user with the privilege to do so.

Summary

Regulators have concerns that laboratory staff could be operating with privileges that allow too much flexibility, or System Policies which are set in an inappropriate way, allowing the opportunity to pass samples which do not meet specifications. It is important for both Regulators and Quality Units to understand software configuration and how it impacts the laboratory workflow as well as the data.

- It is important to understand how Empower System Policies can limit data processing.
- User Types can be setup with very granular privileges to constrain how analysts create results in Review.
- Once results have been generated the associated channels can be locked so that users cannot generate any further results.

- Reviewer User Types can be set up with unique privileges to suit their role which would allow them to view metadata and sign results, but not create or modify results.
- Empower automatically records what was done in the various Audit Trails and users should apply comments to document why it was done.

Neil Lander *is a Principal Product Manager for Informatics at Waters Corporation*

ALCOA+

A	Attributable	*Who acquired the data or performed an action?*
L	Legible	*Can you read and understand the data entries?*
C	Contemporaneous	*Were records documented at the time of the activity?*
O	Original	*Is it the first recorded observation (or a verified, true copy)?*
A	Accurate	*Is the result scientifically valid and error free?*

+	COMPLETE	*All data including any repeat or reanalysis performed*
	CONSISTENT	*All elements of the analysis are date/time stamped and in the expected sequence*
	ENDURING	*Recorded in a permanent, maintainable form throughout its lifecycle*
	AVAILABLE	*For review, audit, or inspection over the lifetime of the record*

Stan W. Woollen, Sr. Compliance Advisor

Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

Backup vs Archive: What's the Difference and Why You Need Both

Dan Chapman

In May 2015, the FDA issued a 483 warning letter to a company after an inspection where its back up strategy was called in to question stating that "without complete, accurate, reliable, or retrievable raw data about the HPLC system's qualification, you lacked complete assurance that the system was operating as intended."[1]

Today, laboratory-based organizations face a wide variety of unaddressed data management challenges, and yet ultimately the scientific data is the currency with which they trade. Proper data management may not pay shareholders but it fundamentally defines the integrity of the organization and it's purpose for existing. Being the cheapest, the fastest or the most definitive is desirable but it is all meaningless if the data is untrustworthy.

Undeniably, along with the continual advancements in analytical technologies comes the ability to generate vast amounts of data. In order to extract the most value from this information, organizations must evolve their data management practices. This change in approach has a direct impact on backup and archiving methodologies.

SHUTTERSTOCK.COM/MAKSIM KABAKOU

Of course data volume is only one part of the story. There are a number of contributory factors that make the plot far more complex, including:

- The need to manage raw lab data under such regulations as 21 *CFR* part 11, Annex11, ISO17025, and the Food Safety Modernization Act (FSMA), among others
- Ensuring potential audits can be readily addressed by optimizing data integrity, searchability and accessibility
- Accomplishing all of this with IT budgets that are flat or declining

Given the requirements described above, organizations desire storage products that provide reliability, long-term retention, searchability of data and low total cost of ownership, without losing the ability to respond quickly in an audit. In this situation traditional back up is not sufficient to meet these needs and this white paper will explain how an archive strategy can:

- Reduce backup and recovery times
- Remove manual intervention and variability
- Minimize exposure during an audit

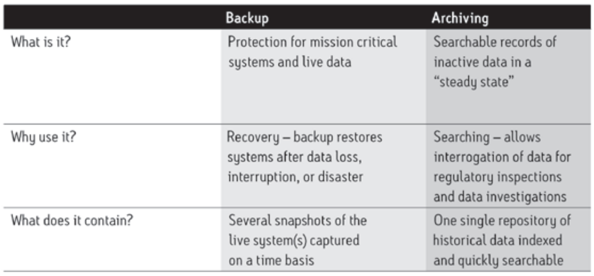
Backup vs. Archive

A classic backup application takes regular snapshots of data in order to provide a means of recovering records that have been deleted or destroyed. Most backups are retained only for a few days or weeks as later backup images supersede previous versions. The best way to think of backup is as a short-term insurance policy against an unforeseen disaster; backups help recover information and processes in current use in case they are interrupted, corrupted, or lost.

Archives serve a very different purpose to backups. They preserve inactive information as required by regulations or company policies. An archive is designed to provide fast search and access to years of information and as a result can aid in the discovery of information not currently in use, in case they become useful again to prevent duplicate work or meet an unanticipated regulatory need. In science-driven industries, results and data integrity can be challenged at any time and even inactive documents may need to be retained for many years.

42% identified archiving and extracting data as an obstacle in their labs.[2]

Archived records can exist outside the traditional backup cycle for a long period of time because by comparison the data is quite static. Meanwhile, the regular backup is protecting live data that is changing on an everyday basis. That does not mean you hold records forever – the best archive solutions also allow you to manage data and documents that are no longer required. This is a critical point – information that should have been deleted could represent a risk to the business given that all data contained in the backup is subject to inspection. But if an effective archive solution is in place,



	Backup	Archiving
What is it?	Protection for mission critical systems and live data	Searchable records of inactive data in a "steady state"
Why use it?	Recovery – backup restores systems after data loss, interruption, or disaster	Searching – allows interrogation of data for regulatory inspections and data investigations
What does it contain?	Several snapshots of the live system(s) captured on a time basis	One single repository of historical data indexed and quickly searchable

Table 1: Backup and archiving at a glance Backup Archiving

data can be automatically flagged and destroyed according to regulations or company policies.

Backups Are for Disaster Recovery – Archives are for Data Searching

Is an archive necessary? A backup is not an archive. If you try to use backups as an archive to support an audit you will soon see a few reasons why this is not recommended:

There are too many backup copies. Backups help to recover systems so you take multiple snapshots of the same data. Explaining which one is valid over another and which is actually the raw data to an auditor can be challenging. In contrast an archive provides a single "official" indexed record.

You cannot search a backup. In order to search a backup, you have to restore the whole thing, in contrast, an archive gives you the ability to search surgically – quickly getting to the data you need and restoring that and that only.

Backups can increase the risk to your organization. If you use your backup as an 'archive', all data will be categorized based on the date you backed it up. Separating data for legal hold and/or managing the lifecycle of individual data sets is impossible and opens the business up to unnecessary risks. With an archive you can make this distinction.

"Legal hold" increases your storage. Continuing from the previous point, if you have one file under legal hold in your backup then it means you have to keep the whole backup and that wastes a lot of storage. An archive allows you to flag only the documents needed and delete the rest when the time comes (e.g. data end of life, mergers and acquisitions).

The impact of archiving spans science, operations, and compliance. A good archiving solution will automatically determine if data is in use or idle and then move that data from expensive high performance storage to more economical archive storage. Furthermore, indexing that archive and its metadata allows for swift search and retrieval when it is really needed without IT assistance, and legal hold will protect that data from accidental deletion or loss.

For example, NuGenesis® Scientific Data Management System (SDMS) allows scientific data generated in your laboratory to be accurately and automatically captured, indexed, and securely stored in a compliance-ready environment immediately after its creation or change. Often this is combined with the Empower® Chromatography Data System to manage inactive LC data.

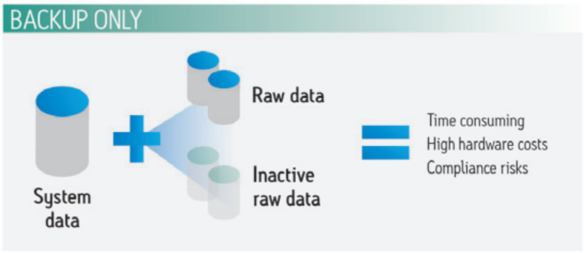


Figure 1: Backup efficiency gains by using an archive solution. Without archiving, much of the time, bandwidth, and storage spent on backup is simply wasted.

Professionals spend over 500 hours annually reviewing and routing files and another 150 hours looking for incorrectly filed documents. It costs $120 to search for a misfiled document, and, if you can't find it… It costs approximately $250 to recreate a lost document.[2]

Managing the mad panic urgency of regulatory inspections can disrupt IT groups and scientists in the execution of their daily project duties. Archives prove their worth during the first regulatory inspection but even without any such requirement; they pay back quickly by simplifying and reducing the IT burden on backup processes.

Conclusion

Backups and archives perform separate functions but the capabilities of each one help the other work better and more efficiently.

Implementing an archive is an efficient, comprehensive approach to managing and protecting laboratory data. Science-driven industries can use an archive in addition to backup solutions to address the growing data volume, regulatory requirements and technological complexity found in the contemporary laboratory environment.

When an archive solution is in place backups run faster, consume less time, energy and system resources, which means better protection for mission critical systems such as Empower.

References

(1) FDA Warning letter http://www.fda.gov/ICECI/EnforcementActions/ WarningLetters/2015/ucm448433.htm 2. IQPC Laboratory Informatics: Current Trends & Predictions for 2015.
(2) IQPC Laboratory Informatics: Current Trends & Predictions for 2015.

Dan Chapman *is a Principal Product Manager for Informatics at Waters Corporation*