LCGC®

JULY 2023

Managing Risk and Digital Data Integrity

- Data Integrity Pitfalls
- Performing a Risk-Based Audit Trail Review
- How to Avoid FDA Citations

This custom ebook is sponsored by ThermoFisher Scientific and presented in partnership with *LCGC*.

ThermoFisher SCIENTIFIC

Driving Data Quality and Ensuring Compliance Using Modern CDS Solutions

By Peter Zipfell

The most safe and effective therapies demand the highest data quality.

Pharmaceutical organizations are responsible for ensuring their therapeutic products meet strict criteria to assure safety and efficacy. The best way to achieve this is through accurate and reliable data obtained from a repertoire of analytical tools throughout the manufacturing process. Recognizing the importance of this process, global regulatory agencies have set strict guidelines to ensure data quality and integrity,[1-4], defined by FDA as data that are complete, consistent, and accurate.[1]

The road to high-quality data is not exempt from obstacles along the way. The growing complexity of novel therapeutic modalities is complicating the manufacturing process, the volumes of data being generated are expanding exponentially, and all of this is

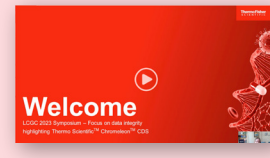
occurring in a regulatory landscape that shifts significantly and at short notice. Failing to ensure high quality data, however, has profound consequences for pharmaceutical organizations and patients—from costly product recalls and reputation damage to ineffective or even unsafe medicines reaching the point of care.

In light of this, several enabling tools and strategies have emerged to help pharmaceutical companies navigate a path to better data. One of the most important innovations that have transpired are advanced chromatography data systems (CDS) that help organizations meet dynamic regulatory requirements while also increasing operational efficiency.

Advanced Compliance Tools Shorten the Path to Data Excellence

CDS are generally defined as the tools that integrate with chromatographic equipment (and, more recently, mass spectrometry systems) to collect, process, and store associated data. The 1970s saw the first iteration of CDS platforms, which grew rapidly in complexity and capability over the proceeding decades.

Today, the latest systems integrate with a suite of analytical instruments beyond chromatography and support pharmaceutical manufacturers to achieve greater data quality. They do so by optimizing operations across five key areas: data acquisition, audit trails, data investigation, data reporting, and system access and permissions.



VIDEO

Carrying Data Integrity into Electronic Records

Optimizing Data Acquisition—Getting Quality Data the First Time

Ensuring high-quality data acquisition starts with effective validation and control of analytical instrumentation. The latest generation of CDS are helping here in several critical ways.

Quelling Qualification Concerns

Accurate, reliable results are not possible unless instrumentation, equipment, and software have been properly qualified. Accordingly, as with manufacturing equipment, analytical equipment qualification is demanded by regulatory bodies.

Considering this, some modern CDS now have functionality and tools that streamline qualification processes while better ensuring compliance to regulatory requirements. For example, comprehensive qualification procedures, both for the CDS and analytical instruments, are now being built into modern CDS platforms. For instruments, these procedures span installation qualification (IQ), operation qualification (OQ), and performance qualification (PQ). They can accommodate a wide range of instruments and vendors

and, in some CDS, are also fully automated. Automating the process better ensures compliance with regulatory requirements while also expediting the process. With such tools, qualification can now be achieved in a matter of minutes.

With the latest systems, qualification results are stored in electronic format inside a secure folder architecture so that no data is ever lost, and a complete historical record of executed procedures is always available.

Improving Instrument Control

While most mass spectrometry and chromatography workflows are broadly the same, they can differ in key details like instrument conditions, sequence structure, and how results are calculated. This can be a source of data quality loss, as tweaking the workflows manually is time-intensive and thus can lead to errors. Advanced CDS are addressing this issue with automated workflow procedures. With them, analysts can create sequences based on defined structures that comprehensively capture all aspects of a workflow and align with regulatory requirements.

Sequence execution control delivers added data confidence in some CDS solutions. In this case, software checks the instrument configuration, methods, and sequences, and prevents a sequence from starting if any issues are detected. With this being run prior to all injections, only correct and consistent injections can proceed, meaning generated data are more reliable.

Delivering with System Diversity

The challenges mentioned previously can be complicated further by the fact labs often operate multiple instruments from different vendors. Idiosyncrasies in instrument operation and the additional burden on staff to accommodate them can open new avenues for data quality loss. A broader trend seen in modern CDS solutions, however, is enhanced compatibility with a range of analytical systems from different manufacturers. The Thermo Scientific Chromeleon CDS, for example, can accommodate more than 540 instrument modules from over 21 different manufacturers.

Benefits here expand beyond data quality and include reduced training requirements, greater ease-of-use with a more consistent end-user experience and streamlined administration and IT infrastructure (although these could be argued to indirectly impact data quality, too, by reducing process complexity and thus risk of error).

On the Trail to Better Data

Beyond the analytical instrument, its sequence, and the results it generates, data reliability, and confidence require a comprehensive audit trail. An audit trail can be defined as a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record.[1] Essentially, they constitute rich information on who did what, when, and why, and are a highly

effective means of detecting data integrity issues. For this reason, audit trails are a regulatory requirement and come under heavy focus from inspectors.

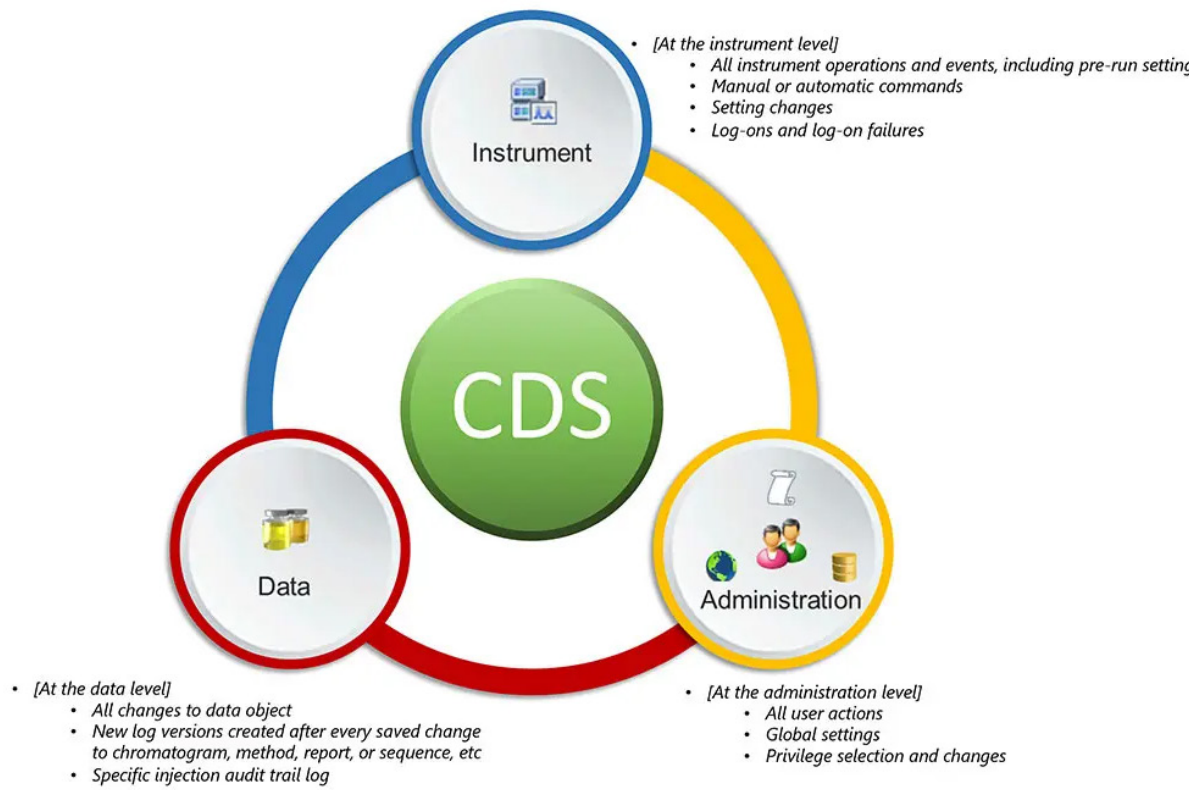
While their importance is evident, building, reviewing, and maintaining compliant audit trails is not so straightforward. For success, audit trails must be set up and configured correctly, undergo time-intensive reviews from quality assurance departments, and easily demonstrate when non-desirable activities have occurred.

Tracking the Who, What, and When

Modern CDS solutions can now comprehensively track the who, what, and when of pharmaceutical manufacturing and testing operations. The most advanced solutions accomplish this by tracking data, covering everything from instrument configuration and data processing to system administration (FIGURE 1).

These tools also facilitate easier review using intuitive filtering options, type-as-you-go or drag-and-drop searching

FIGURE 1. Modern CDS Solutions Now Have the Capability to Capture and Store a Broad Range of Data in Secure and Searchable Audit Trails



functions, and data grouping capabilities, simultaneously with helping create rich and compliant audit trails.

Tracking the Why

Tracking the "why," or the intent, of actions across pharmaceutical testing operations has been considerably more difficult than tracking the who, what, and the when. However, it is a problem that requires serious attention, as the reason for an action provides critical context to data and helps ensure data integrity. Without knowing the 'why' behind an action, those reviewing the data cannot fully reconstruct and understand the events that have taken place, with some resulting in a misunderstanding.

Thankfully, modern CDS solutions have significantly eased the path to accurate and reliable 'why' capture, primarily by enhancing traditional CDS comment functionality. To help capture the 'why' of an action, most standard CDS let users add free form comments. These CDS may even provide a list of default or acceptable comments for the user to select from. However, freeform comments are uncontrolled and can be inaccurate or misleading. Further, the selection of acceptable comments given to end users often spans all possible comments, not just those relevant to the action undertaken. Thus, an acceptable comment can easily be attributed to the wrong action.

Modern CDS solutions overcome this by forcing users to use default or acceptable comments that are tied to specific actions; only the comments applicable to the action in question are available for selection. These pre-approved, action-specific comment options can also be aligned with what is deemed acceptable in a standard operating procedure, meaning users cannot deviate from business acceptance criteria, and compliance is simplified. Importantly, selected personnel can also be given the authority to override default comments if the available options aren't suitable. Carefully controlling and enforcing comments in this way ensures they provide true, complete, and accurate context to actions. Ultimately, this increases clarity, reliability, speed, and confidence when it comes to review or investigation.

Without knowing the 'why' behind an action, those reviewing the data cannot fully reconstruct and understand the events that have taken place, with some resulting in a misunderstanding.

On top of enforcing action-specific comments, modern CDS also ensure user attribution of actions is accurate, namely by requiring input of a password and ID before actions can be completed. While user-session timeouts offer a certain degree of safety in ensuring that actions

are attributable to the correct user, there is still a window of time where another user could complete an action under the wrong login. Passwords and ID requirements eliminate this risk. This feature is important, as performing an action under the wrong user-session, even if accidental, is considered fraudulent activity by regulators. Regulators could mark such activity as an audit observation at the very least, and the broader reliability of data could be thrown into question.

Empowering Thorough and Efficient Data Quality Monitoring

A recent and significant change in regulatory behavior means it is now up to the end-user to defend their data and prove that there are no irregularities. For this, pharmaceutical companies need to be able to monitor and investigate their data easily and at all times.

Within the modern CDS toolkit, there are several solutions that can help pharmaceutical organizations meet this new obligation. Given the heavy workload of quality assurance and quality control personnel, these tools also often prioritize ease-of-use and minimize training requirements.

WHITE PAPER

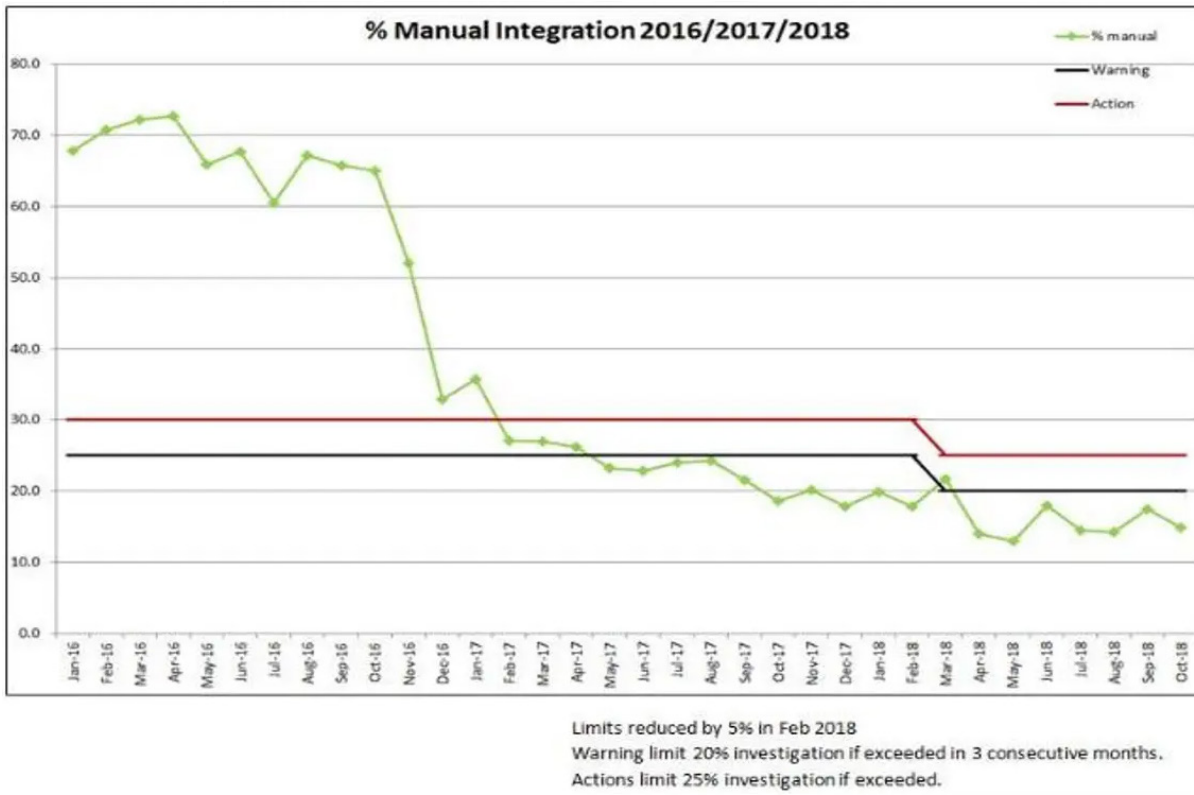
From data integrity regulations to Pharma 4.0

First, advanced version control capabilities allow clearer and faster data change comparisons, whether changes are additions, deletions, or modifications. Such version tracking is accompanied by clear visualizations of changes, and users can revert to previous versions where a change is not acceptable or accurate, meaning issues can be resolved before they have a chance to grow. In some cases, visual comparison features can directly compare versions on a single screen, side by side, providing deeper insight into change, and supporting a clearer justification of changes to regulators. To avoid becoming a source of error itself, the review of comparison panes can be done in read-only mode so that further changes to the data are not possible.

Querying and trending functionalities further build out the modern CDS data monitoring toolkit. CDS with these functionalities can streamline the search for certain types of activity with appropriate search criteria, for example, pinning down all manual integrations or all activity by a specific user in a specified time frame. If the CDS has trending capabilities, graphs and charts can simplify pattern detection, providing a clearer, more succinct summary for regulators (FIGURE 2). Further, with fuller visibility of trends in, for example, user-behavior, laboratories can better implement corrective action before regulatory review.

FIGURE 2. Modern CDS Solutions Effectively Trend Captured Data to Support Proactive Issue Resolution

Here, a high incidence of manual integrations was observed and then rapidly corrected.



Even with these features, finding all the events that could have influenced a data's integrity during review can be a very complex and difficult task. This is because some events are not explicitly tracked or visible from within the audit trail itself, and so searching multiple audit trail entries is needed. Because these events are not prominently displayed or are problematic to identify, they may go overlooked.

Manual integrations and frequent sequence restarts are common examples of such events, with the latter being particularly difficult to identify. To identify and track a sequence restart, for example, a detailed investigation is needed, where a reviewer must look at the sequence start and abort entries and then confirm whether it was the same user carrying out the actions. Such actions could collectively represent a non-conformity when mapped

against business procedures. On the other hand, a thorough investigation could show that the actions were justified.

The latest CDS solutions can search across audit trails and combine specific, related entries, treating multiple operations as one to highlight specific events. This makes it possible to generate a real-time notification when these events occur, alerting team members to actions and operations that are not initially visible from the dataset or object they are reviewing. Further, this trail of events, as with standard audit trails, can be easily searched, queried, and reported on. With this critical additional information to hand, a reviewer has greater visibility, can better recognize patterns, and can be reassured that a more complete and considered audit trail review has taken place.

Straightforward Reporting, Easier Validation

The data analysis journey ends with the reporting of results for product batch release. The traditional reporting processes itself, however, can sabotage data quality. For example, in such processes, data are typically exported to external spreadsheets manually, which, aside from being time consuming, is prone to data transcription errors. Changes to reporting templates and spreadsheets also often cannot be tracked in traditional approaches, so opportunities to detect errors are reduced. Then, when source data change, it can be difficult to ensure reported data reflect the updated results. Further, the use of independent systems for analysis and reporting entails extra software validation burden.

The latest CDS solutions can search across audit trails and combine specific, related entries, treating multiple operations as one to highlight specific events.

More recent CDS address these common pain points by enabling reporting from within the software. With a single system encompassing both data analysis and reporting, there is no need to manually export results, and software validation effort can be reduced. Critically, all changes and versions can then be tracked within the CDS to ensure complete visibility. If any changes start to invalidate a report, then the creation of a fresh one is enforced before submission. Managing the electronic report as it goes through review and final sign-off is also made more robust, namely through unique user-specific digital signatures at successive submission, review, and approval stages.

With less error in electronic reports, better-tracked changes, and enforced control of document review, batch results become more consistent and compliant.

Advanced CDS Tools: Better Data for a Safer World

Delivering safe and effective medicines to patients is the greatest responsibility of pharmaceutical organizations, but it can't be achieved without high-quality data. Several trends are convoluting the path to data excellence, such as an explosion of novel therapies, more complex manufacturing processes, and regulations that shift at short notice.

Among the solutions addressing these challenges is a new generation of advanced CDS. CDS have come a long way since their inception more than five decades ago, maturing considerably into the advanced solutions seen today. With the latest platforms, pharmaceutical organizations can better drive quality and efficiency at all stages of the data collection, analysis, and reporting journey while better weathering regulatory change. The result is more reliable data, higher quality medicines, and, ultimately, a safer world.

References

1. FDA, *Data Integrity and Compliance With Drug CGMP: Questions and Answers Guidance for Industry* December 2018.
2. FDA, *CFR Part 11, Electronic Records; Electronic Signatures - Scope and Application* September 2003.
3. MHRA, *'GXP' Data Integrity Guidance and Definitions* March 2018.
4. EMA, *Guidance on Good Manufacturing Practice and Good Distribution Practice: Questions and Answers* (2018).

Peter Zipfell
Marketing Manager
Thermo Fisher Scientific

ThermoFisher SCIENTIFIC

Built for **stability.**
Built for **performance.**

Why compromise?

Thermo Scientific™ Chromeleon™ 7.3.2 Chromatography Data System delivers vast improvements in performance, compliance, and overall usability while increasing the resilience of network operations. With greater processing power and additional network structure, the entire CDS performance is amplified while providing IT with all the tools for security, stability and maintenance without compromising the needs of the lab.

It's the best Chromeleon CDS yet.

Learn more at
thermofisher.com/chromeleon

thermo scientific

A Harmonized Approach to Performing a Risk-Based Audit Trail Review

By Julie Lippke, Joseph Mongillo, Thomas Cullen, Christian Metz, Katria Harasewych, and Fouad Benamira

The IQ Working Group has defined a pragmatic risk-based approach to audit trail review, where it is only required for high impact GxP data

Audit trail review (ATR) is a mechanism to detect potential critical changes to data/system security settings and to ensure the quality and integrity of reported data. The authors have defined a risk-based approach to ATR where ATR is only required for high impact GxP (good manufacturing practices [GMP] and good laboratory practices [GLP] for the purposes of this paper) analytical data and possible system security changes. This approach requires a fully documented risk assessment that encompasses the technical controls and identification of data impact. Note that while analytical data are the focus of this paper, the principles outlined may be applied to other activities.

Regulatory Expectations

Data integrity, particularly electronic data integrity, has become an area of increased regulatory focus. Per FDA[1]: "For purposes of this guidance, audit trail means a secure, computer-generated, time-stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record."

In 2018, the United Kingdom's Medicines & Healthcare products Regulatory Agency (MHRA) and the US FDA issued guidance documents on the topic. MHRA's *'GXP' Data Integrity Guidance and Definitions* was issued in March 2018. FDA's *Data Integrity and Compliance with Drug CGMP—Questions and Answers* was issued in December 2018. These documents join guidance issued by the World Health Organization (*Guideline on Data Integrity*) and the Pharmaceutical Inspection Convention Pharmaceutical Inspection Co-operation Scheme (PIC/S, *Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments*).[1-4]

The publication of these guidance documents is associated with enforcement actions with an emphasis on data integrity that stem from a failure to follow current good manufacturing practices (CGMPs) predicate rules and existing regulations in 21 *Code of Federal Regulations* (*CFR*) 211 for electronic systems.[5]

PIC/S *Good Practices For Data Management And Integrity In Regulated GMP/GDP Environments*—July 2021[6]—gives an indication of the key elements to consider for an effective risk-based approach: "Data criticality (impact to decision making and product quality) and data risk (opportunity for data alteration and deletion, and likelihood of detection/visibility of changes by the manufacturer's routine review processes)."

Therefore, regulatory expectations for audit trail review have become an established part of the GxP data lifecycle.

Scope and Intended Use

This article introduces a harmonized approach to performing a risk-based ATR developed by a working group of the International Consortium for Innovation and Quality in Pharmaceutical Development (IQ).

It should be noted that the scope of this article includes electronic instrument analytical data where raw data are stored in non-volatile memory (i.e., can be recalled later). Both enterprise and standalone data acquisition systems are in scope.

Systems that do not generate data are out of scope.

The following terms are defined[5]:

- Technical control—computerized features like audit trail, backup mechanism, user management and security, electronic signatures and/or digital signatures to assist or enforce administrative and procedural controls

- Procedural control—standard operating procedures (SOPs) and work instructions for operation and administration, system user controls, computer system validation, calibration, network qualification, awareness training, etc.
- System controls—combination of procedural and technical controls for a system.

Risk-based Approach

Recent regulatory guidance such as those from FDA and MHRA emphasize the implementation of risk-based approaches to ensuring data integrity. The FDA guidance reminds us that[1]: "CGMP regulations and guidance allow for flexible and risk-based strategies to prevent and detect data integrity issues."

Similarly, the MHRA guidance describes[2]: "a risk-based approach to data management that includes data risk, criticality and lifecycle."

The concept of performing a data integrity risk assessment specific to a particular data acquisition and processing system is laid out in the MHRA guidance[2]:

"An example of a suitable approach is to perform a data integrity risk assessment (DIRA) where the processes that produce data or where data are obtained are mapped out and each of the formats and their controls are identified and the data criticality and inherent risks documented."

The data integrity risk assessment is seen as a driver of compliance and prioritization of any necessary remediation activities. While audit trail review is often considered an essential part of ensuring data integrity, the same guidance clarifies that routine data review should include a documented audit trail review *where this is determined by a risk assessment* (emphasis added) (2).

BLOG

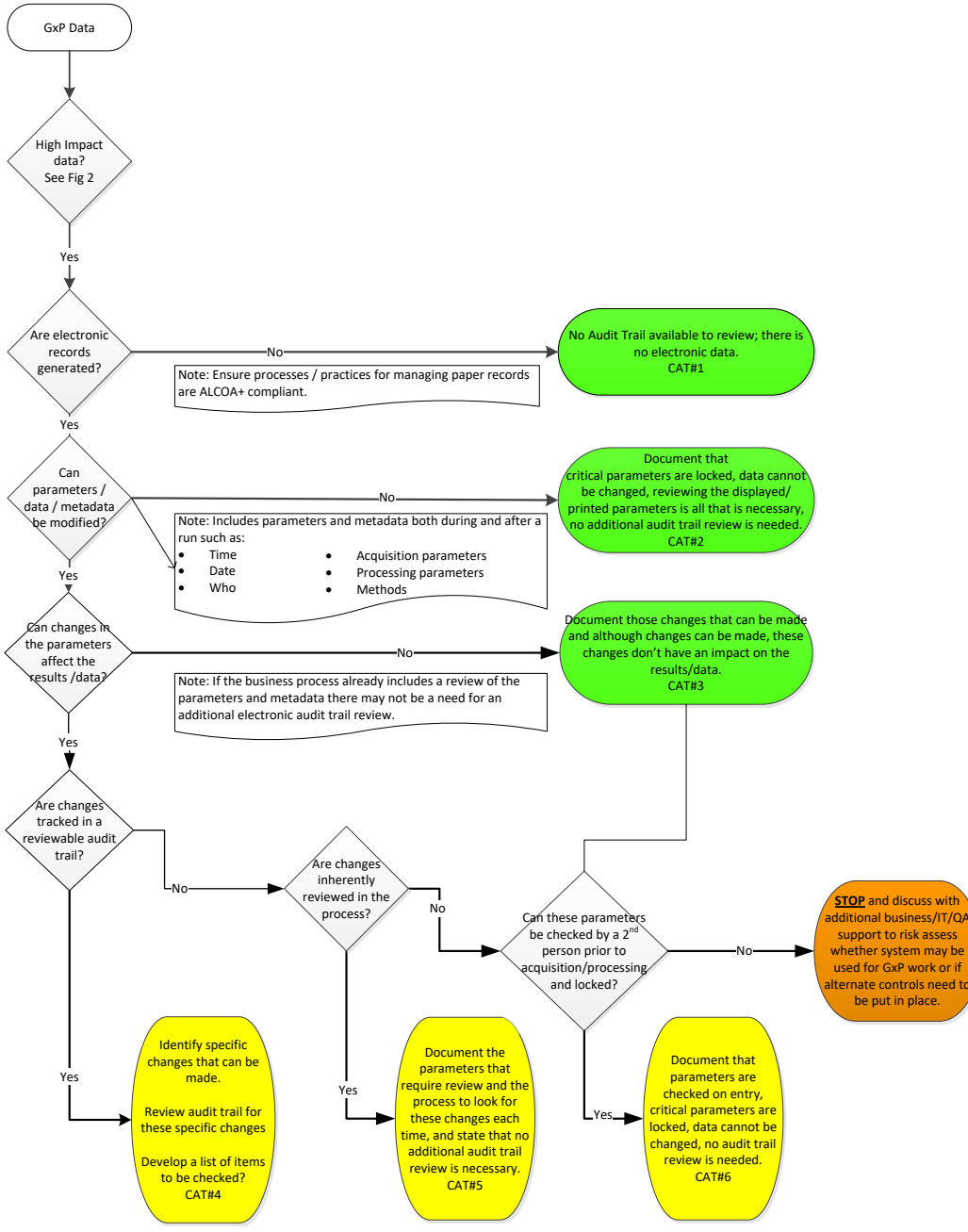
Quality Risk Management: Know the Risks

The appropriateness of any mitigation of a data integrity risk should be assessed in the context of the criticality of the gap. MHRA defines critical risks as those that impact the potential of data or metadata "to be deleted, amended, or excluded without authorization." FDA states[1]: "Data integrity is critical throughout the CGMP data lifecycle, including in the creation, modification, processing, maintenance, archival, retrieval, transmission, and disposition of data after the record's retention period ends."[1]

It should be noted that archival and retrieval are out of scope for this paper on ATR.

A decision tree has been developed (FIGURE 1) where data types were categorized and the need for audit trail review considered. This serves as a risk assessment that can be used

FIGURE 1. Risk Assessment Tool for Determining Audit Trail Review Requirements. Where ALCOA+ is Attributable, Legible, Contemporaneous, Original, and Accurate, Plus the Data Needs to be Complete, Consistent, Enduring, and Available



Categories 1, 2 and 3 are preferred, the acceptability of categories 4, 5 and 6 are dependent on the risk tolerance of a company as well as the availability of alternative compliant instruments (1).

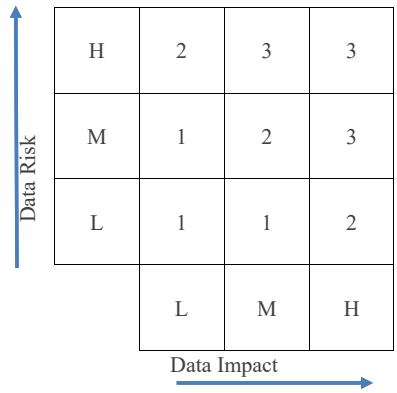
to determine the need for procedural controls, and the controls should be documented within the qualification package for new equipment or in change management system for equipment updates. A risk assessment, for instance the one described in *Assessing Data Integrity Risks in an R&D Environment*,[7] may be used to define data integrity elements for a system where audit trail review is the chosen mitigation. FIGURE 1 is specific to ATR and does not include data review. For GLP, data review and ATR need to happen at the same time, for GMP there may be opportunity to separate and streamline some activities with a documented risk-based approach.

Determining the Need for and Frequency of ATR

Data Risk—ATR should be considered for electronic GxP relevant data when a technical control does not remove the need to review the audit trail. A risk-based approach should be applied to ATR, and this general approach is described in FIGURE 2. Tools such as the risk filtering tool in International Council for Harmonisation (ICH) Q9[8] may be used.

When possible, there is a preference to implement technical controls to reduce/eliminate the need for ATR. It is preferred

FIGURE 2. Determining the Rigor of Audit Trail Review (ATR) as a Function of Data Risk and Data Impact



LEVEL	AUDIT TRAIL REVIEW EFFORT LEVELS
1	No ATR is required, as supported by a documented risk assessment. ATR is performed on a "for cause" basis only.
2	ATR may be performed on an *ad-hoc* basis or periodically at a pre-defined interval.
3	ATR must be performed as part of the broader data review prior to the release of the data.

to prevent an undesirable action from occurring if this is technically feasible. In cases where prevention is not possible, detection of the undesirable action through data review (including ATR) is required. In rare (limited) cases where an action may be neither prevented nor detected, discuss with additional business/IT/quality assurance (QA) support to risk assess whether the system may be used for GxP work or if alternate controls need to be put in place such as a procedural control.

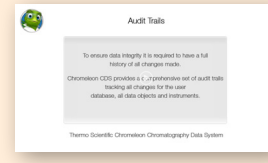
It is preferred that a technical control be employed to prevent data deletion. If deletion cannot be prevented, the ATR process should be designed to detect that specific activity. It should be noted that, in many cases, ATR is most logically performed concurrent with other data review activities. The severity of any residual risk should be assessed. The frequency for ATR should be commensurate with the probability of the risk occurrence. The frequency may be adjusted based on documented historical performance.

Intended Use of the Data—The intended use of the data should also have an impact on the need for and frequency of ATR. The data's potential risk impact on patient safety and product quality should be considered, and GxP-relevant data are determined by regulatory requirements.

High risk impact data are defined as data with potential for direct impact to product quality and patient safety. Individual companies may identify other activities as high impact but at a minimum would include release, clinical stability, and cleaning verification.

While it is acknowledged that companies may assign slightly different levels of impact to the same data types, some useful guidance may be obtained from an informal poll conducted of IQ member companies. Data arising from activities such as GLP studies, cleaning verification, clinical product release, and stability were considered greater impact and may trigger ATR. Activities such as method validation may have an indirect effect on product quality and patient safety and may be less impactful and have a medium/low impact dependent on a company's risk considerations.

Defining Appropriate ATR Effort/Frequency—Together, the assessments of the system characteristics and limitations and the impact of the data's intended use will facilitate identification of records, steps, and changes, and enable risk classification (low to high) and a tiered audit trail review effort.



VIDEO

Audit Trails

Performing Data ATR

A decision tree describing the performance of ATR is provided in FIGURE 1. Additional explanatory comments about the decision tree are given as follows.

Where it is possible for changes to be made to the experimental conditions, metadata, or other parameters that have the potential to affect the results/data, one control strategy to ensure detection is to perform ATR. In these cases, the following should be considered as critical changes (and potentially included in a list of elements to be checked):

- Changes to test parameters
- Changes to data processing parameters (analytical method)
- Deletion of data
- Repeated analysis or reprocessing without justification
- Change history of finished product test results
- Changes to sample sequences
- Changes to sample identification
- Changes to critical process parameters.

The requirements for ATR (and data verification in general) should be proceduralized and should define requirements on a software-by-software basis dependent on the assessed data risk and impact. The frequency and responsibility for ATR should be defined in the procedure. Evidence of audit trail review should be documented, in most cases by defining the meaning of the overall review signature.

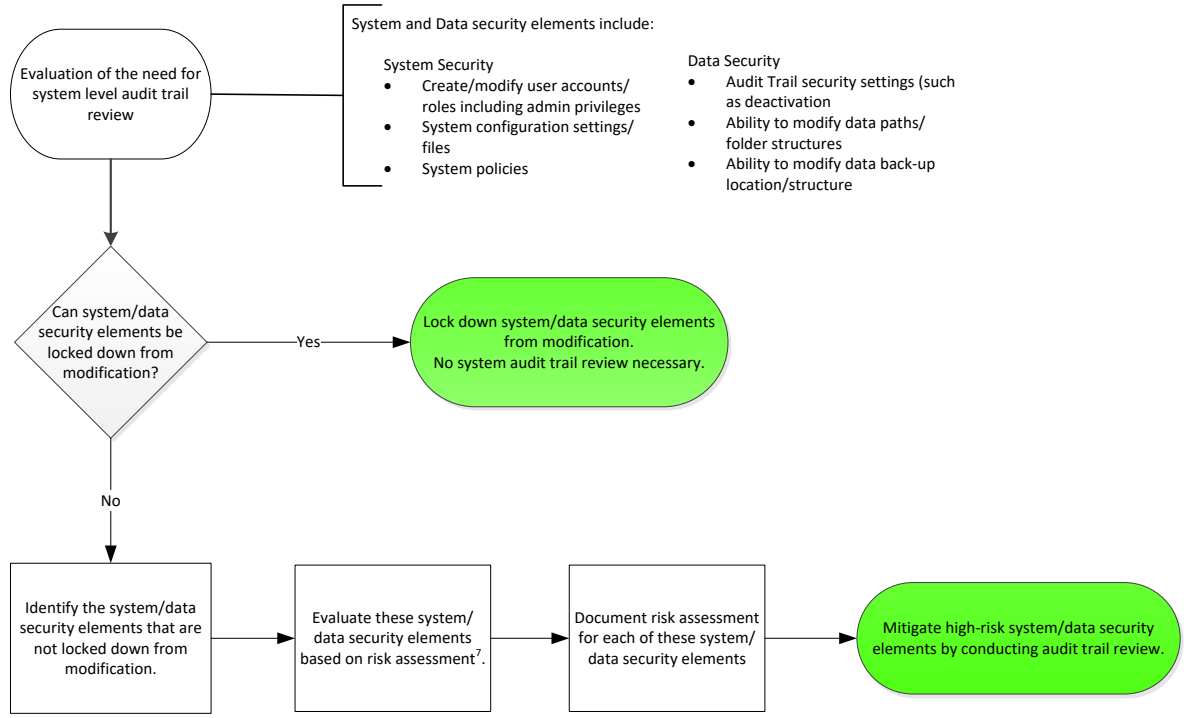
System Level ATR

The purpose of a system level ATR is to ensure key configurations and settings have not been changed (either intentionally or unintentionally). It is recommended that the system audit trail (which contains, for example, system administrator actions such as deletion of data or changes to system security settings) also be reviewed at least periodically. This periodic review will ensure the system has remained configured as it was during validation/qualification. Based on the type of the system and corresponding data, the following items might be considered:

- System policies
- Deactivation of audit trail
- Changes to data paths or folder structure
- Changes to reports or calculations
- Data security management (lifecycle including archival, restoration, etc.)
- Audit trail review may be used to verify appropriate access privileges have been used. Other processes may be employed to satisfy this requirement such as user access reviews (including admin privileges)
- Configuration files
- Library files (where applicable) where the technical controls of the library would drive the need and frequency for review.

A decision tree has been developed (FIGURE 3) for system-level ATR where data types were categorized with examples and the need for audit trail review considered.

FIGURE 3. Decision Tree for Determining Minimum System Level Audit Trail Review Requirements



(7) J. Lippke, et. al., "Assessing Data Integrity Risks in an R&D Environment," *Pharm. Technol.* 44 (8) 51–53 (2020).

Appropriate Audit Trail Comments

Manually entered audit trail comments should be suitable for an auditor/inspector to read and should include the scientific rationale for why the change was made. GAMP 5[9] provides audit trail requirements for an audit trail entry. Note: There may be character limitations, so it may be necessary to document justification outside of the electronic system and include a cross-reference. Manually entered comments will also require review and should be contemporaneous (within a reasonable experiment/review time frame). If time has elapsed, then the time gap should be supported with a justification.

Conclusion

ATR is a mechanism to detect potential critical changes to data and one means to ensure the quality and integrity of reported data. The authors have defined a pragmatic risk-based approach to ATR where ATR is only needed for high impact GxP data and that ATR can be targeted to focus specifically on critical changes that may be possible.

This approach requires a fully documented data risk assessment that encompasses the technical controls, identification of relevant high-risk impact data, which may vary on a per-organization basis. The preferred approach is to utilize technical controls wherever possible.

ATR inherently remains a manual process that is resource intensive, and opportunities for automated data transfer/digitalization removes opportunity for critical changes negating the need for ATR where utilized. In addition, when a system has been configured to provide visual flags for undesirable actions/states, or when the audit trail provides filtering or searching capabilities, these abilities may be leveraged to streamline ATR.

References

1. FDA, *Data Integrity and Compliance with Drug CGMP—Questions and Answers* (Rockville, MD, December 2018).
2. MHRA,*'GXP' Data Integrity Guidance and Definitions* (London, UK, March 2018).
3. World Health Organization, *Guideline on Data Integrity* (Geneva, Switzerland, October 2019).
4. PIC/S, *Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments* (Geneva, Switzerland, November 2018).
5. US *CFR*, Title 21, Food and Drugs (Government Printing Office, Washington, DC), Part 211.
6. PIC/S Guidance PI 041-1: *Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments* (July 2021).
7. J. Lippke et al., *Pharm. Technol.*, 44 (8) (51–53) (2020).
8. ICH, Q9 *Quality Risk Management* (ICH, Geneva, 2005).
9. ISPE, *GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems* (February 2008).

Julie Lippke and **Joseph Mongillo** both work in Analytical Research and Development at Pfizer Inc. (Groton, CT); **Thomas Cullen** and **Christian Metz** both work in Analytical Research and Development at AbbVie Inc. (North Chicago, IL and Ludwigshafen, Germany, respectively); **Katria Harasewych** works in Computer System Validation Quality, CoE at Merck & Co., Inc., (West Point, PA); **Fouad Benamira** works in Analytical Development Sciences for Biologicals at UCB S.A. Belgium. All contributors are part of the IQ Working Group.

ThermoFisher SCIENTIFIC

Built for **learning.**
Built for **you.**

Chromeleon University

The Chromeleon University has been designed to support you as a software user, whether you are new or an experienced user. Search for resources to leverage key techniques and applications, with over 300 videos, on-demand webinars, spotlights, and technical notes to assist you and your laboratory.

Register to access the Chromeleon University!

Learn more at
thermofisher.com/chromeleonuniversity

thermo scientific

How Are You Going to Prevent or Solve This Data Integrity Mess?

By R.D. McDowall, PhD

Strategies for compliance and best practices in chromatography labs

Data integrity continues to be a major concern in GXP regulated laboratories since the Able Laboratories fraud case in 2005.[1] The purpose of this article is to discuss some key data integrity topics facing regulated chromatography laboratories and how to resolve them. Instead of learning from the best, we will learn from the worst laboratories using FDA citations. We will look at ways to avoid ending up in the same mess. We will focus on the data life cycle from acquisition, processing, interpretation, reporting, and preservation throughout the record retention period.

What Do the Regulators Want?

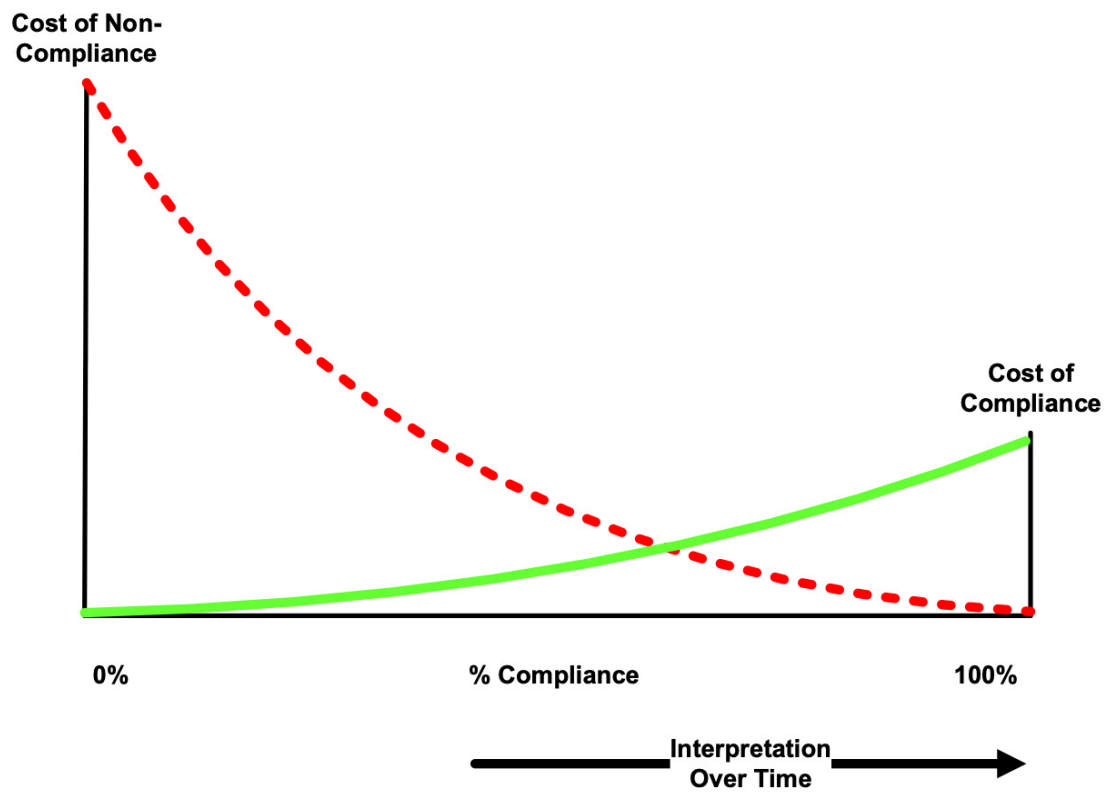
The GMP regulations for laboratory records are simple: 21 CFR 211.194(a) requires *complete data*.[2] The phrase is simple to

interpret: everything. All data generated during the analysis including sample preparation records, chromatograph set up, analysis, peak integration, calculation of the final results, errors, and instrument problems. These data are reviewed by a second person to ensure that work was performed correctly and there are no poor data management practices or falsification.[3] All data must meet ALCOA+ criteria[4-6] and be attributable, legible, contemporaneous, original (or a true copy), accurate, complete, consistent, enduring, and available. A recent European GCP guideline has added a tenth criterion of traceable for ALCOA++.[7]

Understanding the Costs of Compliance and Non-Compliance

It is important to understand the costs of compliance and non-compliance; these are the costs of creating a system that encourages user compliance and a right-first-time mindset with proper justification for activities versus having to investigate, redo work, and build in justification later. This mentality is built on structured risk management and the difference in approach to remediation cost is demonstrated in FIGURE 1.

FIGURE 1. Understanding the Costs of Compliance and Non-Compliance[9]



No matter how the level of compliance is established, as noted by the arrow in the bottom right, interpretation of regulations will change. For example, there is no mention of audit trail review[2] in US GMP (21 CFR 211), but since the Able Laboratories fraud case[1] audit trail review is a regulatory requirement.[5,8] The ultimate message is that the cost of compliance is always cheaper than the cost of non-compliance.

User Accounts and Data Integrity

In an audit or inspection of a CDS, user account management is often the first place to start. Therefore, this part of a CDS needs to be configured in a way to support user requirements but not allow activities that present high non-compliance risks such as users having administrator rights or deletion privileges.

Shared Accounts

Are your CDS user licenses too expensive and do you want to save money? One solution is to share user accounts and passwords. However, your return on this lack of investment comes when it is found during an inspection: no attribution of action to a named individual. How good do those savings look now?

A way to avoid this problem is to evaluate the license model of the CDS—named user versus concurrent user. Named user requires one license for each user of the system. For a laboratory with 30 chromatographers, you'll need 30 licenses. In contrast, with a concurrent license model, this is the maximum number of users you can have logged onto the system at any time. Thus, from the pool of 30 users, you may need only 15 licenses for the same laboratory.

Some laboratories will argue that a shared generic read-only account is acceptable, as users cannot change any data. However, the audit trail captures logon/logoff activity and any "generic" user account, even read-only, is an indicator that users can perform activities in the system without being attributable. The best advice is to avoid it.

Default Accounts

Software applications have a default account that is used to set up and configure the application. A typical username and password combination may be *admin*/*admin* and may be printed in the user manual. The only function intended for the admin account in a compliant configured software is to create named user accounts at initial installation, and this may include any work that the supplier's service engineer conducts, such as interfacing of chromatographs and execution of qualification protocols. Once handed over to the laboratory, it is good practice for the IT administrator to create their own administration account and disable the default and service engineer's accounts.

Access Privileges

A well thought out access privilege system should have no conflicts of interest between roles. For example, it is good practice for administrators to not have user privileges and vice versa. QA reviewers should have read-only access to oversight activities.

No user should have deletion privileges. This ensures that an analyst cannot remove inconvenient results. A second person reviewer avoids the need for checking the audit trail for deletions and simplifies audits and inspections.

Chromatography Data and Records

Once named accounts with the correct access privileges have been set up, we can start doing some chromatography analysis. However, there are some data integrity areas that needs to be navigated to avoid regulatory problems later.

Paper Printouts Are NOT Raw Data

There are still laboratories together with QA departments that fail to recognize that *complete data*[2] includes the electronic records used to generate the signed paper printouts. See questions 10 and 12.[5] Indeed, this has been the case since FDA posted on their web site in 2010[10] the rationale for saying paper printouts were not a *true copy* (as per 21 CFR 211.180(d)) of the electronic records generated during the analysis and interpretation of the sequence. Furthermore, a paper printout of the analysis was not an *exact and complete* copy (as per 21 CFR 211.68(b)) of the underlaying electronic CDS records including the sequence file, acquisition and processing methods and audit trail.

The citation from the Intas Pharmaceuticals 483 observation [11] in December 2022 illustrates the problem:

> *Paper printouts are used as the raw data for <redacted> analysis…During reconciliation of analysis performed on January 12, 2021, for instrument SC1111, printouts could not be provided for review* (for stability test injections).

To avoid such problems the definition of complete data or raw data must include all electronic data and associated metadata within the CDS plus any printouts from the system if it is proceduralized to be used as a hybrid. The capture method and media may be dependent on several internal procedures but some typical requirements include:

- **All chromatography data files**—blanks, standards, samples (including any reinjections due to expected or unexpected events) associated with the whole sequence
- **Metadata used to acquire these data files**—instrument file, sequence file, (including sample identities, dilution factors, purities of standards, sample weights, and so on) along with acquisition parameters
- **Metadata used to process these data files**—processing method, modifications

to the processing method applied to all injections in the sequence and manual repositioning of baselines—only if permitted by the laboratory peak integration SOP
- **Metadata used to monitor changes**—all audit trail entries associated with creation and modification of data including peak integration associated with the analytical run (*note: no laboratory user should have deletion privileges*)

This leads us to the next area of regulatory focus, peak integration.

Peak Integration Potential Problems

The Intas Pharma 483 has a peak integration citation that is comprised of several issues:[11]

- No procedure for describing manually entered integration events
- Analysts are permitted to manually enter (any) integration events and reprocess the chromatograms
- Reviewers only check the final and not original integration
- A procedure exists for Interpretation of Chromatograms that requires manual integration to have a reason and approval by a section head. But this does not apply to reviewing for frequent adjustment of integration events
- Changes were found to have been made to either the samples or the standards, but not both
- The ability to adjust integration events resulted in batch results that would have triggered laboratory investigations meeting specifications, such as:
  - Changes to fronting and tailing sensitivity to an impurity in the samples but not the standards allowed a batch to meet specifications
  - Use of minimum area reject in samples reduced the number of reportable impurities
  - When reprocessed under the inspector with consistent integration parameters across the whole sequence these batches were out of specification (OOS).

There was no mention of CDS audit trail review findings in the 483 form for the company, but a *cascade of failure in the Quality Unit* was mentioned.[11] Unsurprisingly, a warning letter was issued in July 2023.[12]

Peak integration must be carefully controlled to avoid the perception that users are or can intentionally bias the results to circumvent having to redo work. A flexible CDS product requires built in tools that consider that:

1. Chromatography is a comparative and not an absolute analytical technique. This means that all standards and samples in a sequence must be integrated using the same parameters and the software should prevent and indicate where this is not the case to reviewers.
2. Changes to a processing method must be retained and the differences

between versions be determined of what was changed, when, and by who with justification for why captured in procedures, experiment records, or system required comments.

3. Depending on the analytical procedure, a CDS should have tools to reduce risk through product control. For example, restricting the modification of integration events for the quantitative method of the active ingredient would reduce the risk to review cycles for that method. This is in contrast to a method for impurities which typically requires more user flexibility but consequently would require a higher level of procedural control.

VIDEO

Data integrity challenges

Regardless of the extent of controls that can be used it is important that all attempts at integration is captured in the audit trail and that reviewers are aware of and trained to find these events. As noted by part of the answer to Question 12 of the FDA Guidance Data Integrity and Compliance with Drug cGMP:[5]

> *FDA expects processes to be designed so that data required to be created and maintained cannot be modified without a record of the modification. For example, chromatographic data should be* ***saved to durable media upon completion of each step or injection (e.g., peak integration or processing steps****; finished, incomplete, or aborted injections) instead of at the end of an injection set, and* ***changes to the chromatographic data or injection sequence should be documented in an audit trail****. Aborted or incomplete injections should be captured in audit trails and should be investigated and justified.*

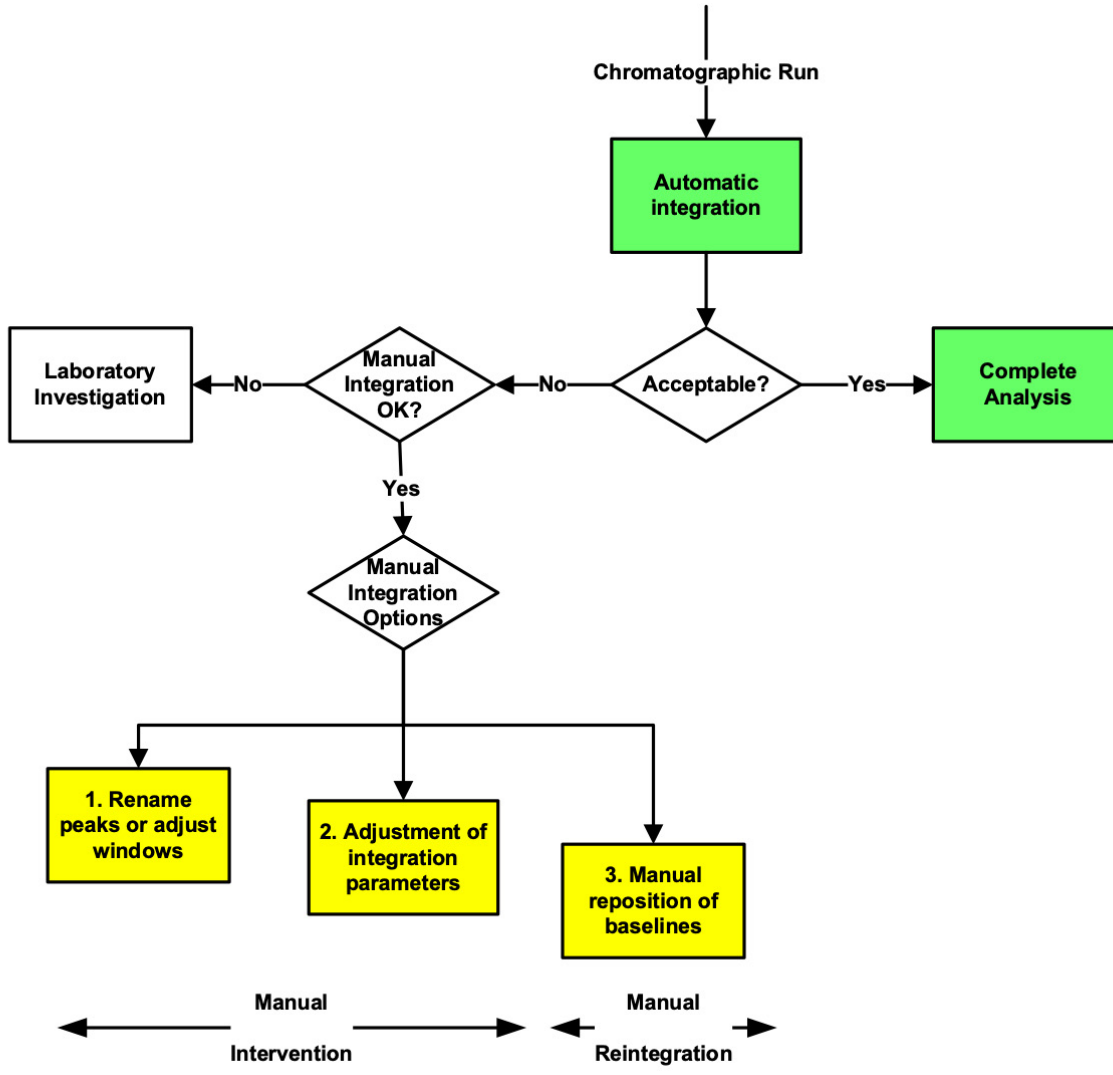
Therefore, each integration iteration must be saved and the changes recorded in the audit trail.

To help control peak integration, a flow chart is presented in FIGURE 2. It differentiates manual integration (manual positioning of baselines) from manual intervention (changing of integration parameters).[13] All changes need to be considered for use case in a method and risk-assessed if they are or are not acceptable actions, in what circumstances, and defined for how to review and document them. This brings us to the review of such entries, which is a regulatory requirement[8] and regulatory expectation.[4-6]

Challenges with Audit Trail Review

A critical part of a second person review of chromatography data is the audit trail review. It is vital that reviewers define acceptable, risk-assessable, and unacceptable actions that users would perform for methods. From

FIGURE 2. Flow Chart for Manual Intervention and Manual Integration[13]



that assessment, a quality CDS system would provide tools for reviewers to leverage the audit trails that are produced from those actions during batch record result review.

The first challenge with approaching audit trail review is the understanding the differences between 21 CFR 11 and Annex 11 regulations for audit trail:

- Part 11 requirements cover *create, modify, and delete* data[14]
- Annex 11 requirements target *GMP relevant changes and deletions*[8]

For an effective risk-based review, Annex 11 is more comprehensive to procedural review and focuses on changes to data. Any technical controls that a CDS has where data changes are highlighted or keyword searches that can identify key events such as abort run, altered processing method, or moved baseline must be used to the full extent. Where a change event is identified it should be possible to drill down and assess what was changed to see if it is a significant event or a normal action by an analyst. Where necessary, the electronic action such as abort run should have a corresponding entry in the instrument logbook.

Implicit is the fact that audit trail review must be conducted electronically. Personally, the review should be conducted either with a large enough screen (or two screens) to have the chromatography data in one window and the audit trail in another. Please resist the urge to print the audit trail for review. Printing an audit trail produces a file that is representative at the time of printing and is not considered a complete audit trail review since audit trails are dynamic. For example, consider the case where a printed copy is filed with the records, but actions such as additional electronic signatures are added to the sequence after printing the audit trail; this could be perceived by regulatory reviewers that the files are being changed after review and not in control. Printing and signing audit trails can complicate your process, slow your review, and introduce errors or regulatory questions into your practices.

It is highly recommended to utilize product control wherever feasible, for example, users should not have deletion privileges to reduce the burden of reviewers needing to search for deletion. As another example, configuring locked storage areas with specific user access in the database so that working areas are predefined and cannot be changed will reduce the amount of system wide data that should be considered during review.

Protection of e-Records Over the Record Retention Period

One of the classic FDA warning letters highlights the problem of the laboratory backing up their own CDS data. Often it is done only when the staff have time, which is rarely. Ohm Laboratories last backup their CDS data about six months before an inspection and when asked why, they said they did not have sufficient time. This leads to two citations for one observation:[15]

- Failure to protect records
- Failure to have adequate staff numbers

Following approval of the reportable result, all associated records must be locked so that the data can be viewed by authorized users but not changed. If there is a complaint, then records can be unlocked, and any investigation work carried out and the data e-signed again and locked.

For longer-term record retention, data can be archived in a secure and resilient location to reduce the volume of data backed up by IT. Data can then be retrieved and imported

easily by an IT administrator for further work to be undertaken.

Summary

We have reviewed some of the common data integrity problems that can result in regulatory citations. Avoiding many of these are common sense and good IT practice such as having sufficient user licenses for attribution of action, not sharing accounts, disabling the default account, and having IT perform the backups. Controlling peak integration is a case of good analytical science, as chromatography is a comparative technique. Audit trail review should be performed electronically on each batch before release as an integral part of second person review. And finally, we touched on record retention needs to ensure that the records are stored in a secure manner but can be retrieved when required.

References

1. *Able Laboratories Form 483 Observations*. 2005; Available from: https://www.fda.gov/media/70711/download.
2. *21 CFR 211 Current Good Manufacturing Practice for Finished Pharmaceutical Products*. 2008, Food and Drug Administration: Sliver Spring, MD.
3. *Amendments to the Current Good Manufacturing Practice Regulations for Finished Pharmaceuticals.* Federal Register, 2008. **73**(174): p. 51919 - 51933.
4. *WHO Technical Report Series No.996 Annex 5 Guidance on Good Data and Records Management Practices*. 2016, World Health Organisation: Geneva.
5. *FDA Guidance for Industry Data Integrity and Compliance With Drug CGMP Questions and Answers* 2018, Food and Drug Administration: Silver Spring, MD.
6. *PIC/S PI-041 Good Practices for Data Management and Integrity in Regulated GMP / GDP Environments* 2021, Pharmaceutical Inspection Convention / Pharmaceutical Inspection Cooperation Scheme: Geneva.
7. *EMA Guideline on Computerised Systems and Electronic Data in Clinical Trials*. 2023, European Medicines Agency: Amsterdam.
8. *EudraLex - Volume 4 Good Manufacturing Practice (GMP) Guidelines, Annex 11 Computerised Systems*. 2011, European Commission: Brussels.
9. R.D.McDowall, *Do You Really Understand the Cost of Noncompliance?* Spectroscopy, 2020. **35**(11): p. 13-22.
10. *Questions and Answers on Current Good Manufacturing Practices, Good Guidance Practices, Level 2 Guidance - Records and Reports*. 2010 22 Dec 2019]; Available from: https://www.fda.gov/drugs/guidances-drugs/questions-and-answers-current-good-manufacturing-practices-records-and-reports.
11. *Intas Pharmaceuticals Limited Form 483 Observations. Available from: https://www.fda.gov/media/164602/download*. 2022.
12. *FDA Warning Letter Intas Pharmaceuticals*. 2023, Food and Drug Administration: Silver Spring, MD.
13. R.D.McDowall, *Where Can I Draw The Line?* LCGC Europe, 2015. **28**(6): p. 336-342.
14. *21 CFR Part 11; Electronic Records; Electronic Signatures Final Rule.* Federal Register, 1997. **62**(54): p. 13430 - 13466.
15. *FDA Warning Letter Ohm Laboratories* 2009, Food and Drug Administration: Rockville, MD.

R.D. McDowall, PhD
Owner, McDowall Consulting