Data Integrity:
Technical controls that demonstrate trust

Using Chromeleon 7 Chromatography Data System for enhanced data integrity

Author

Shaun Quinn, Marketing Manager
Informatics and Chromatography
Software, Thermo Fisher Scientific

Keywords

Data integrity, compliance, integrated informatics, enterprise CDS, enterprise data management, GMP, GLP, GCP

Summary

An increased focus on data integrity by international regulatory agencies has led to serious consequences for several companies. It has also resulted in data integrity becoming one of the top reported global issues that regulated companies face. Data governance is an integral part of a regulated company's quality system, of which, data integrity is fundamental. As such, manufacturers and analytical laboratories are required to design and operate a system which provides an acceptable state of control based on data criticality and inherent risk.

A chromatography data system (CDS) that provides the functionality to achieve compliance is a vital partner in data integrity. Having a CDS that has been implemented appropriately and is managed correctly, with all of the necessary preventative and detection technical controls, built-in to one package that are easy to use, demonstrates a level of trust.

Thermo Fisher
S C I E N T I F I C

Table of Contents

Introduction

Medicines are unlike many other products. When you pick up a medicine, how do you know that it is going to work properly according to its intended purpose? In most cases you can't tell that, so it is all about trust; having faith that the manufacturer has produced a product that is fit for its purpose. Regulated life science companies make decisions that impact their product quality every day and base those decisions on the data that they generate. Patients are therefore dependent on regulated companies having confidence in the quality and integrity of that data.

Data integrity is a fundamental element of a regulated company's quality system and is not a new concept and dates back decades. However, data integrity has become increasingly a primary inspection point of perspicacious inspectors, which has caused a visible increase in data integrity findings across all geographies.

If facing a data integrity focused inspection, the emphasis is on providing evidence that the analytical results are not fraudulent. According to the Medicines and Healthcare Products Regulatory Agency (MHRA), "data integrity requirements apply equally to manual (paper) and electronic data." However, for many, they have already made the transition from paper-based processes to electronic. Electronic data is deemed more secure, reduces human oversight, is more difficult to manipulate or change, and any such changes easier to detect. This perception of electronic data is based on an assumption that the software has the technical controls to support compliance with 21 CFR Part 11 and that those technical controls are appropriately implemented and managed.

There are components of Part 11 that are not meant to be satisfied by technical controls within a computerized system. For example, §11.10(j) of 21 CFR Part 11 states: "The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification." This is a requirement that a chromatography data system will likely never satisfy. Therefore, it should always be understood that data integrity controls for electronic records are not limited to just technology and tools.

However, where procedural controls are put in place to plug gaps in a system's ability to support the technical controls necessary to achieve compliance with the regulations, human nature means that these procedural controls may not be adhered to, and in such situations, a technical control is the only means of remediation to negate the human element. It is this point which is pertinent to understanding the impact of the latest data integrity guidance on software such as a Chromatography Data System (CDS). The CDS must provide the required technical controls and ideally those controls should be preventative but where that is not feasible then there must be controls that can detect problems.

This paper is therefore focused on identifying some key aspects of the latest data integrity guidance that are applicable to chromatography data systems and in particular, the preventative and detection controls provided within Thermo Scientific™ Chromeleon™ 7 Chromatography Data System (CDS).

Regulator's guidance

With international regulatory agencies having more focus on data integrity, the Food and Drug Administration (FDA), World Health Organization (WHO), and Medicines and Healthcare products Regulatory Agency (MHRA) inspectors have been trained to better recognize data integrity issues. As a consequence, there have been an increasing number of findings, so all of the agencies have released new guidance on data integrity. The MHRA in UK have already released their guide "GMP data Integrity Definitions and Guidance for Industry" (March 2015). The WHO also released their guide "Guidance on good data and record management practices" (May 2016). The FDA has released "Data Integrity and Compliance With CGMP - Guidance for Industry" (April 2016) which is still in draft mode at time of writing this white paper but has been on comment rounds and is expected to be finalized in the near future.

All of the documents provide a definition of data integrity: "The extent to which all data for its entire lifecycle is complete, consistent, and accurate." (MHRA). The World Health Organization and Food and Drug Administration add to it using the principles of ALCOA and ALCOA+:

• Attributable: who acquired the data or performed the action

• Legible: can you read and understand the data entries

• Contemporaneous: documented at the time of the activity

• Original: first recording of data or a true copy

• Accurate: reflects what took place.

The guidance documents also outline the 'red lines' for inspectors which in terms of a CDS relate to review and retention of data, audit trails, user access and rights controls, testing into compliance, and administrative controls.
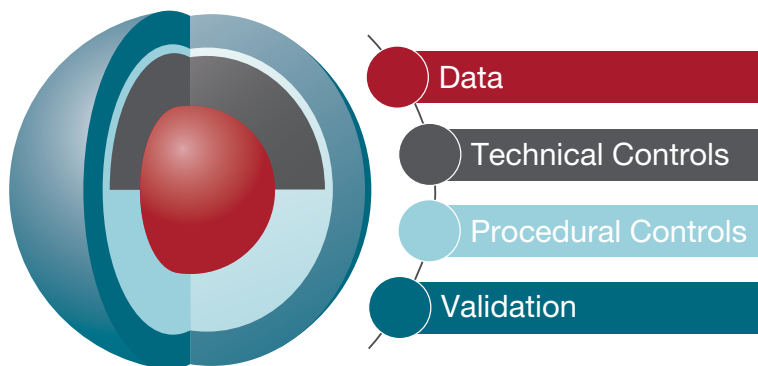

Figure 1. Overview of layers required to ensure integrity of CDS data.

Data review

The Chromeleon CDS architecture has always provided users with an easy means to review data. The Sequence contains an injection list and maintains the order in which injections are analyzed; it includes the injection results (chromatographic raw data), associated methods such as Instrument Method, Processing Method, Report Template and Spectral Library. It incorporates metadata, including all versions of all objects, with complete auditing to describe the full history of the sequence. Having this level of containment gives reassurance and an easy means to look at final results and work through the data and understand the process of by whom, when, and why any changes were made. Using the version comparison tool of Chromeleon CDS you can dynamically establish all changes that have been made, for instance, to an Instrument Method (Figure 2).

Figure 2. The Chromeleon CDS Modification history tracks all changes to all data objects and lists the before and after state of each variable associated with each change.

Audit Trail review

According to the MHRA: "When designing a system for review of audit trails, this may be limited to those with GMP relevance (e.g. relating to data creation, processing, modification and deletion, etc.)". Chromeleon CDS has always had extensive audit trails and segregates them according to their relevance so that it is easier for users to review and interpret them. The Chromeleon CDS 'Versioning and Data Audit Trails' completely documents important changes and operations performed on specific data objects like Data Vaults, Sequences, Injections, Processing Methods, Instrument Methods, Report Templates, Spectra Libraries and modified Chromatograms. In addition to just tracking changes, it offers the opportunity to view the differences between two versions of a data object. Furthermore, an older version can be reinstated as the current one, by reverting to the older version of the data object.

In terms of data creation, retained with each injection record is the injection audit trail that captures all activity from the instrument during the capture of raw data (Figure 3).
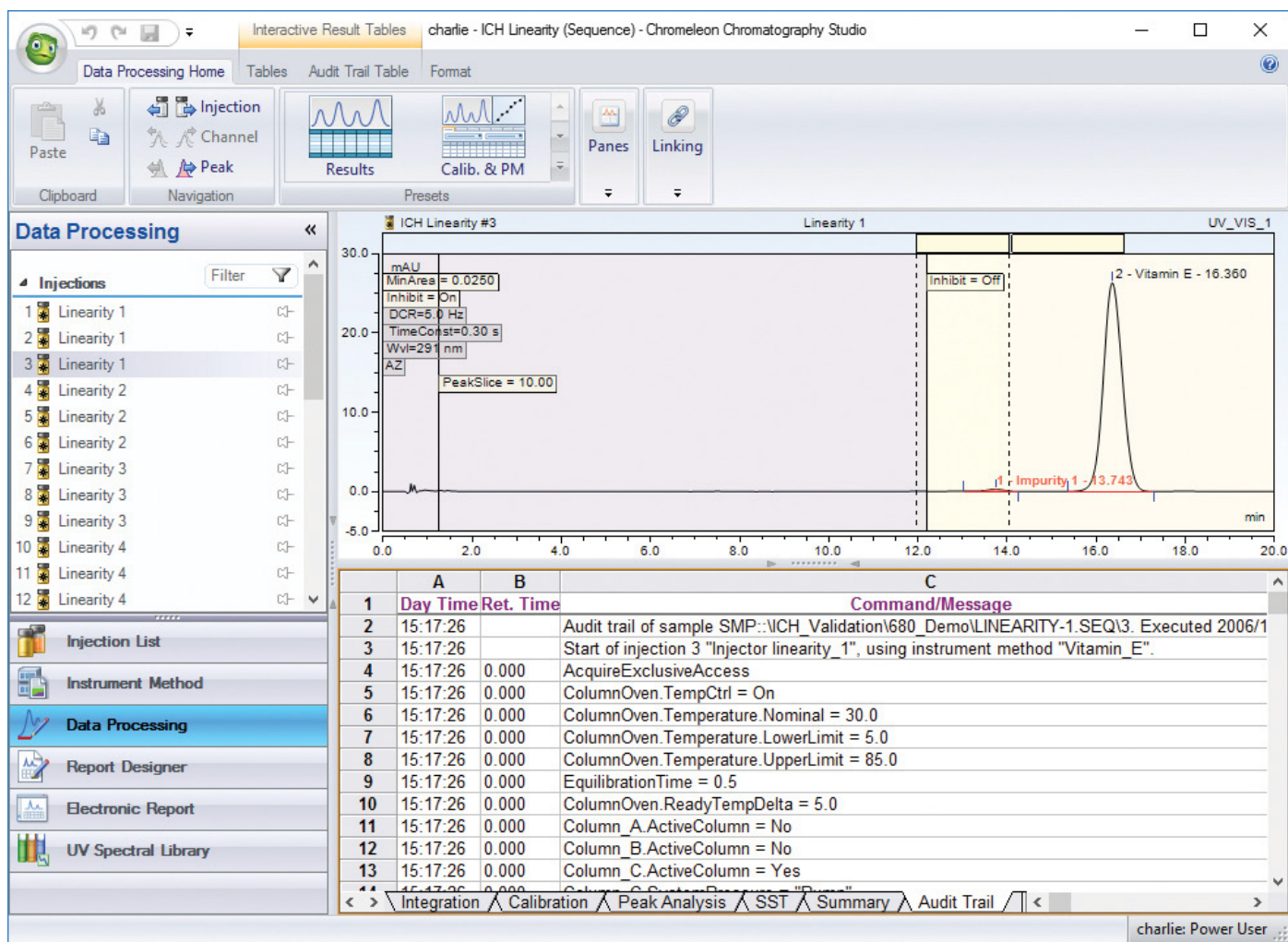

Figure 3. Injection audit trail associated with each injection of a sequence.

For processing and modifications, Chromeleon CDS has a tiered approach to the Audit Trail that allows greater granularity and provides the capability to version data objects. The data audit trails of the respective object provide a history of the current object and, more importantly, Date/Time stamps, Operator ID and the Operation. These are recorded for all events that resulted from the object being modified. In accordance with regulations, record changes must not obscure previously recorded information. Therefore, it is possible in Chromeleon 7 CDS to directly compare the different versions of the object by highlighting the two records of interest and selecting 'Show changes'. This opens the interactive version comparison dialog that highlights where modifications have been made, and directly compares the records showing the values of all old and new records. The structure of versioning provides the capability to easily view changes in depth and also revert back to an earlier record if desired. If the revert action is executed, it is fully tracked in the audit trail and treated as an additional new record. The audit trails also capture the deletion of child objects. The Chromeleon CDS versioning means that you can now restore deleted items with full traceability, such as the example Report Template, as shown below (Figure 4).

Figure 4. Restoring a deleted Report Template.

The latest guidance from regulators also introduces the concept that an audit trail review must be performed and that that action is captured. As stated in MHRA's guidance: "There should be evidence available to confirm that review of the relevant audit trails have taken place." Effectively, regulators are holding computerized system audit trails to a higher standard, for example, during sample preparation when an analyst is possibly performing a dilution step using a pipette, the analysts' attest that they followed the relevant analytical method protocol and associated SOPs but there is not necessarily evidence to confirm they have done it. This is therefore a new requirement that hasn't necessarily been enforced in the past and Thermo Fisher Scientific is working with all relevant parties to better understand how this can be achieved demonstrably with new technical controls.

Shared Logons and Access rights

The Chromeleon CDS security system provides the user management capabilities required to meet the requirements of 21 CFR Part 11 and the latest guidance. No user identities are shared and every user is identified by User Name, Full Name, and Job Title throughout the software (Figure 5).

Figure 5. Users are identified by User Name, Full Name, and Job Title throughout the software and User Names are unique for every user.

The Chromeleon CDS advanced security system supports an unlimited number of security levels and is designed to fit the chromatography workflow. Over 160 different privileges can be allocated as appropriate to an unlimited number of different Roles. A Role is a collection of user privileges that define what the users that have this Role are allowed to do in Chromeleon CDS (for example, Lab Managers would typically be granted privileges to modify integration, whereas Operators might only have privileges to create and run sequences). Two Roles would therefore be created to differentiate between the different tasks. Users can be a member of several roles and choose a Role at logon. The privileges are not cumulative therefore a user is only permitted to perform the actions that have been assigned to the Role they logon with. These allow detailed definitions of privileges for different user groups and allow the same user to perform multiple Roles in a controlled manner.

Forcing individual users to have a unique User Name does not in itself categorically ensure that no user account is ever shared. Someone may attempt to try and use another user's details to gain access or a user might mindlessly share some of their details with someone else. The Chromeleon CDS user management audit trail should deter such activity and provides System Administrators with the means to easily monitor excessive failed logon attempts attributable to a specific user account (Figure 6) or be able to identify if a user is logged on in multiple locations at the same time (Figure 7). Of course, there may be a legitimate explanation for both of these scenarios but backed by procedural control stipulating, for example, that the system administrator should monitor this activity during periodic reviews of the system, the technical controls provide an easy means to identify occurrences and for action to be taken.
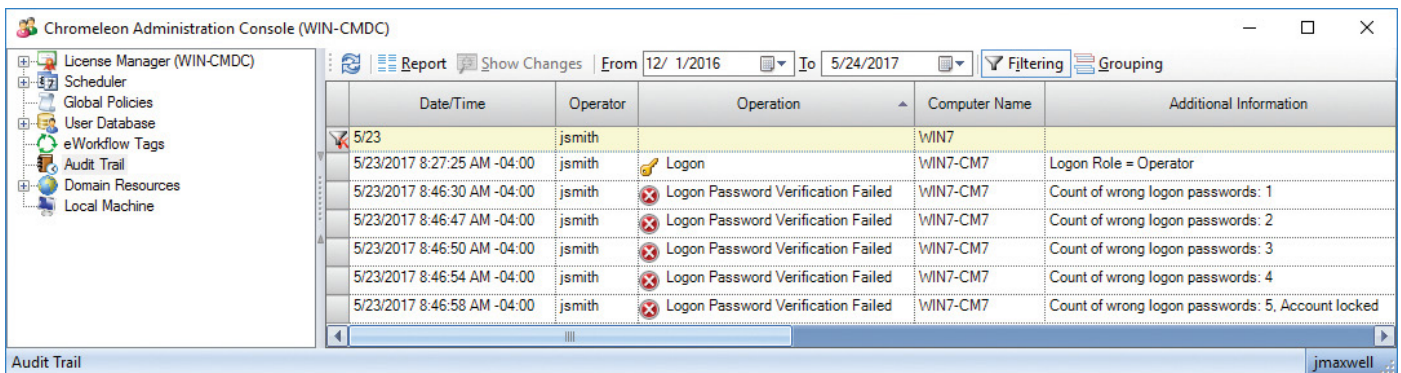

Figure 6. With all logon, logoff and failed logon attempts being tracked and the ability to filter within the audit trail, Chromeleon CDS can assist in identifying activity such as failed attempts to access a locked session.
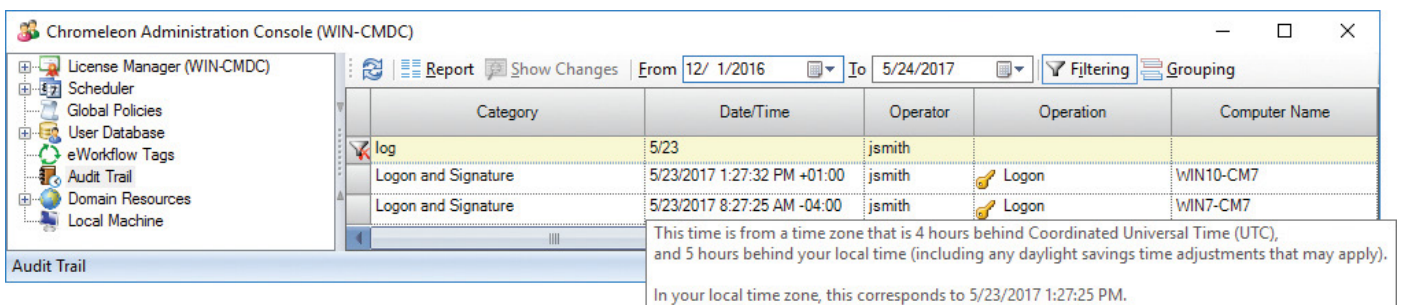

Figure 7. With concise information and easy filtering, activity of user accounts being shared can easily be identified. With the unique time zone tooltip it can be established, for instance, that one user has logged on at the same time in two different regions.

Testing into compliance

A chromatography data system cannot determine what an analyst puts into a vial or verify that it is as claimed or prevent that an analyst uses an actual sample for system suitability, test, prep, or equilibration runs. However, using the Chromeleon CDS privileges and access controls you can limit the ability of users to create sequences that they intend to use for the purposes of testing different samples until they obtain the desired result and then hiding them in a non-descript folder. In addition, a regular search for sequences that have only one or two injections, or sequences that have had re-injections of samples, injections that have been interrupted, injections that have been aborted, or injections that have not been processed can be easily performed (Figure 8). The resulting information from these queries can then be used as a guide to where to look in Chromeleon CDS, in order to further investigate the history behind this data.
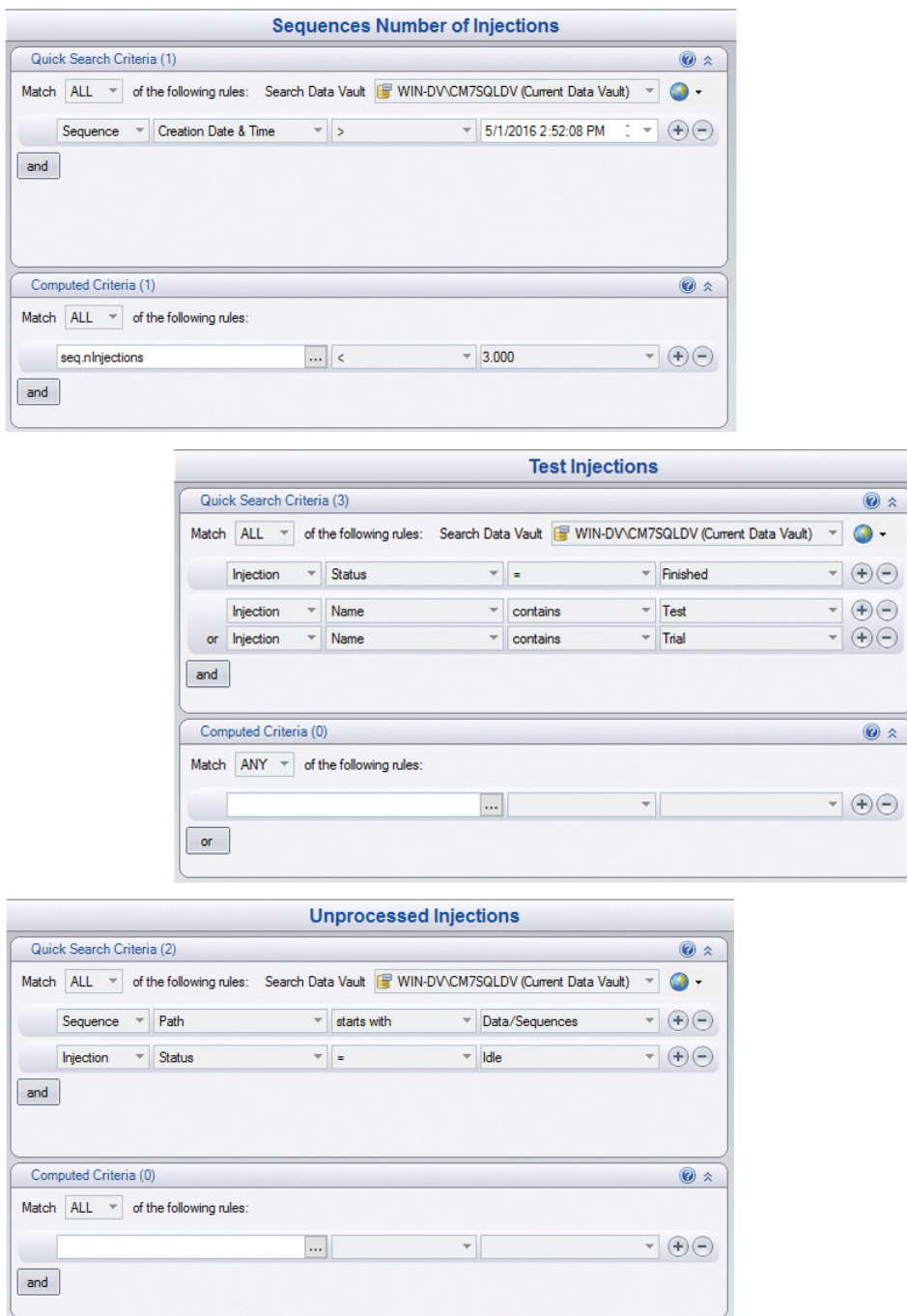

Figure 8. Using the Chromeleon CDS Query function to identify possible actions relating to Testing into Compliance.

It is highly recommended that every laboratory establishes a Standard Operating Procedure (SOP) for chromatographic integration including detailed measures for the use and control of manual integration. In an ideal world every peak would be integrated first time with an absolute minimum number of integration parameters but that simply isn't the reality and therefore, for many users, preventing the use of manual integration using the CDS privilege controls is not an option. To assist with review, all chromatography data systems need to clearly indicate which injections have had any manual intervention. As an additional measure, a review of all manual integration operations should be conducted periodically and an assessment made as to whether manual intervention is being used excessively (Figure 9).
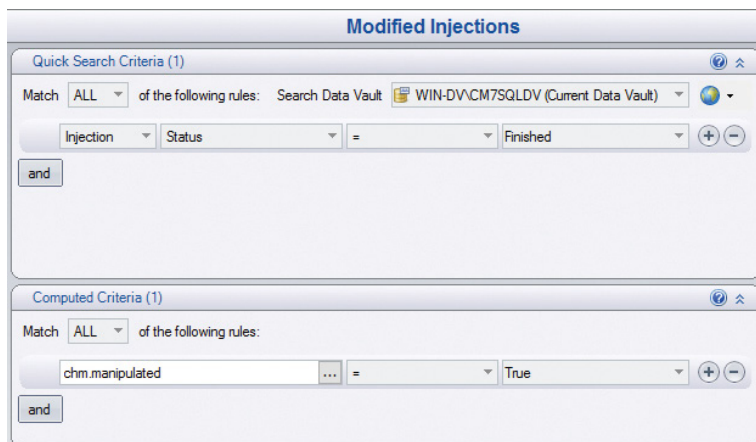

Figure 9. Using the Chromeleon CDS Query function to identify all instances of manual intervention.

System Administrator

With an increased focus on data integrity there is a greater burden on System Owners and Administrators and also greater scrutiny of their management of the system. Although not expressly required in the guidance from the regulatory agencies, Thermo Fisher Scientific recognized that to support System Administrators there needed to be technical controls that can be used to demonstrate effective system management rather than implicitly assuming it, just because they are the recognized system owners. The latest release of Chromeleon CDS therefore has extended its auditing to capture administrative and system events such as instrument configuration, data vault changes, changes to the Chromeleon CDS domain resources, and system events that can happen to the various Chromeleon CDS stations. There are now greater access controls to the administrative components of Chromeleon CDS and even greater security of raw data including audited verification checks should any attempts be made to manipulate data outside of the CDS (Figure 10).
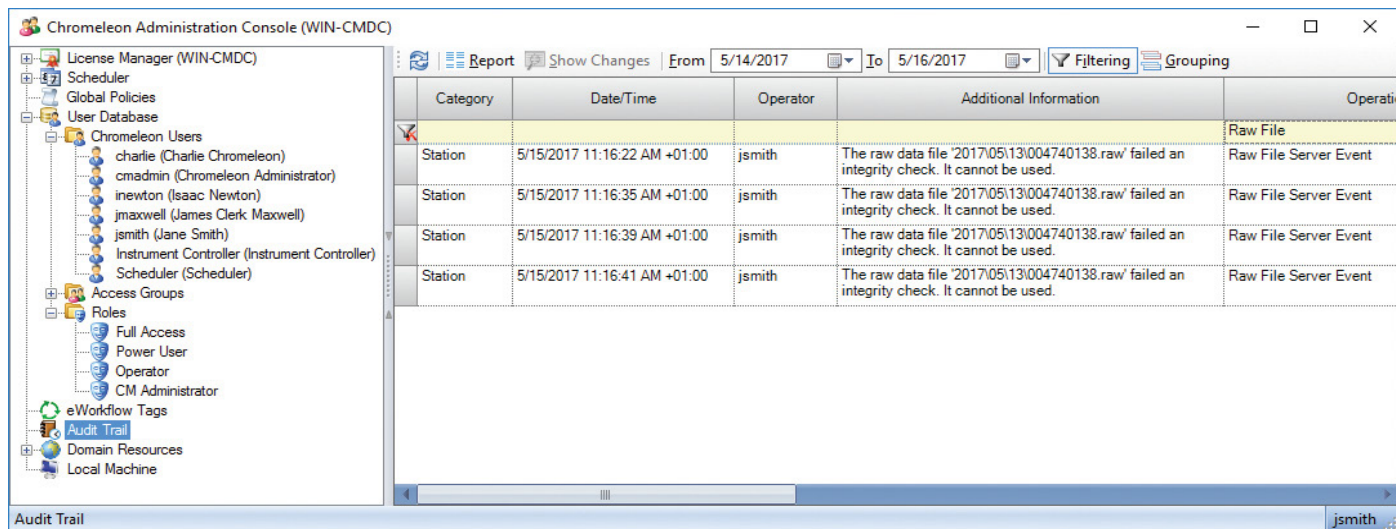

Figure 10. Audit Trail filtered to show raw data file integrity check failures that are captured in Station Audit Trail.

Conclusion

Data integrity fundamentally depends upon a corporate culture that values quality. Accountability for ensuring data integrity runs throughout all levels of an organization and across all business functions, from product development, through manufacture and testing, to product distribution and safety monitoring. A chromatography data system that provides the functionality to achieve compliance is a vital partner in data integrity, but any benefits can be negatively impacted if, for instance, the company does not buy enough user licenses and therefore in so doing encourages users to find alternative means such as the sharing of user accounts. However, data integrity can be protected with the right culture, procedural controls, good validation, educated employees, and a chromatography data system that has all of the necessary technical controls built-in to one package that are easy to use.

Interested in our complete data management solution?
Learn more about the entire Thermo Scientific Integrated Informatics
portfolio at **thermofisher.com/integratedinformatics**

Like Charlie Chromeleon on Facebook to follow his travels and get
important updates on chromatography software!
facebook.com/CharlieLovesChromatography

Visit AppsLab Library for online access to applications for GC, IC,
LC, MS and more. **thermofisher.com/AppsLab**

Find out more at **thermofisher.com/chromeleon**

Thermo Fisher
S C I E N T I F I C