Demystifying Audit Trails in the GMP QC Laboratory

INTRODUCTION:
Everyone who has read recent drug GMP warning letters and forms 483 know that the issue of data integrity remains a high priority among regulatory investigators. And among enforcement actions, the words ‘audit trails’ are mentioned frequently, and have been for over ten years. I will address, at a high level, the purpose and value of audit trails, features that their configuration should ensure, and how they should be managed after they are enabled. Appendix 1 provides a list of some features that should be considered in system configuration to ensure that audit trails are adequate and meet regulators expectations. Appendix 2 provides a sample of eight deficiencies identified in warning letters that mention ‘audit trails’.

CONCLUSION: Validated computer systems with enabled audit trails are necessary, but not sufficient, to meet global regulatory good documentation practices requirements for electronic records. Most commonly used laboratory instrument software programs support their implementation so firms have many options to be compliant in this area. FDA warning letters cite a variety of laboratory software: Empower 3, Chromeleon, SpinChrom and TotalChrom™ just to name a few. Many firms use current versions of these software in a manner compliant with electronic record requirements, suggesting that how audit trails are configured, enabled or not, and utilized in data review is the issue at hand. Alternatively, firms may use a hybrid system to implement audit trail requirements when software may have a specific gap. Audit trails should be configured to identify WHAT action was performed, WHO performed the action, WHEN it was performed and WHY it was performed. These requirements should be identified in ‘user requirements’ and testing should be conducted and documented as part of the validation process.

Implementations of adequate system controls in conjunction with appropriately configured and enabled audit trails is not enough to be compliant with global electronic record requirements. It is also essential to review the relevant audit trail(s) as part of the data verification process. A variety of system controls ensure that complete, original and attributable data are retained. These controls include unique log in password combinations, appropriately assigned privilege functions, fixed date and time stamps, and automatic saving of data as it is acquired. Appropriately configured audit trails provide the meta-data record to confirm that the data used to make GMP decisions are complete and valid. It is only through review of electronic data, including associated audit trails that the firm can determine whether those records are “invalid or altered”. Further, the review of electronic records and audit trails ensures that the Quality Unit considers ALL data, including OOS results, in making lot disposition decisions. Failing to consider invalid or altered records in lot disposition decisions, may result in release of medicinal products that fail to meet scientifically sound and appropriate specifications and may not be safe or efficacious.

Put simply: Electronic records must be supported by adequate audit trails and associated controls that ensure the ‘…ability to discern invalid or altered records.’ The Quality Unit must review these electronic records and associated audit trails to ensure that ALL data are considered in batch release decisions.
BACKGROUND:
Before going any further, it’s worth looking at three definitions. All are very similar in that they identify that audit trails are chronological records that enable reconstruction of events.

- **MHRA GUIDANCE 2015**: ‘GMP audit trails are meta data that are a record of GMP critical information (for example the change or deletion of GMP relevant data), which permit the reconstruction of GMP activities.’
- **FDA, 21 CFR Part 11**: Use of … audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.
- **WIKIPEDIA**: ‘A chronological record of system activities to enable reconstruction and examination of a sequence of events and/or changes to an event’
- **WATERS CORPORATION**: ‘Systematic ‘story’ of the data from creation, through interpretation and final assessment and reporting.’

Before additional discussion of electronic audit trails, consider what the corresponding process would be in an entirely paper based system. We all know how to manage that, simple ‘good documentation practice’. For example, when a staff member makes a mistake in completing information in a paper batch record they follow this process:

1. Draw a single line through the incorrect entry. This ensures that the incorrect result remains readable and is not obscured, is available for review and the information/data are complete and permanent.
2. Enter the ‘correct’ value or information
3. Initial and date the revision. Thus, we know who made the change and when they made it. The information or data are attributable and documented contemporaneous with the action.
4. Provide a justification for the change made to the record or data. For example, this could be because a simple transcription error occurred. Thus, we have some level of confidence that the information or data were not changed simply because someone didn’t ‘like’ the previous information. The information or data are accurate and original.

Consider that the electronic audit trails we talk about here are simply the electronic version of the paper version of line-out-correct-initial-date-justify and should conform to similar expectations.

Now, let’s proceed with the unique aspect of validation requirements for electronic record systems. 21CFR Part 11.10(e) states: Validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records. Unlike other validation efforts for pharmaceuticals including process, cleaning and method validation, electronic system validation requires that we are able to identify invalid or altered records. How do we ensure we have the “…ability to discern invalid or altered records?” Appropriately configured and enabled audit trails are key. Appropriately configured audit trails within a validated electronic system are necessary, but not sufficient, to achieve the goal. Implementation of other controls that we address are necessary to achieve that goal.

Audit trail definitions either specify or allude to their use in allowing reconstruction of activities. Simply put, audit trails should document WHO performed and action, identify WHAT was done,
WHEN it was done, and WHY it was done. Many software options exist for laboratory systems. Most current software systems have been developed with electronic record requirements in mind though their ease of use may vary from one product to another. It is prudent to evaluate the software capabilities, including user friendliness when it comes to audit trial review prior to purchase. It may be that the more expensive product will save analyst and reviewer time, and this is reasonable to factor into the cost equation. And these software systems have many possible audit trails, but those which are relevant for this discussion include: Sample audit trails, Results audit trails, Method Audit trails, Project audit trails and System audit trails.

Other important controls must be in place, in addition to enabled audit trails, for firms to have the ability to ‘discern invalid or altered records.’ These include, for example:

- **The requirement for unique login password combinations** in order to attribute actions to a specific individual. Shared passwords do not permit this attribution and their use makes the audit trail incomplete.
- **All data must be saved and all results addressed.** Data must be saved as it is acquired and not after the fact. Further, failing results should be investigated and determined to be valid or invalid. When retesting is conducted, it should be performed according to a written procedure and protocol.
- **Date and time stamps** should be fixed, ideally at the network level, and analysts should not have access to change them. This ensures that results are not backdated or otherwise made to appear they happened at a different time or date.

Let’s assume your firm has validated computer systems with appropriately configured audit trails so that you know WHO performed an action, WHAT action was performed, WHEN it was performed and WHY it was performed. That means you are good to go, right? Wrong again. The purpose of the audit trail is to ensure that the data generation and processing activities can be reconstructed and that ALL data are available for review. **The underlying concern of regulatory authorities is that not all data are considered in lot release decisions and in the worst case the information that is not considered is either falsified or failed specifications.** So now, these audit trail(s), along with the electronic data they support, must be reviewed as part of the data verification process. Failure to review electronic data, including relevant audit trails has also been cited in many warning letters. See Appendix 2 for examples.

And finally, as data are secured and periodically backed up for protection against a catastrophic event that might result in loss of the data, the audit trails must be included in the back up and retained for as long as the original record is retained.

For those who want a deeper dive into the technical details some of some links are provided. The links are provided in no particular order and no not represent an endorsement of the associated products. Educational courses from Waters may be found [HERE](#). Understanding Empower Audit Trails, starting [HERE](#) on slide 56. The tabulation of Part 11 requirements regarding audit trails for Agilent ChemStation are provided [HERE](#) starting on page 3, section 11.10(e.). Perkin Elmer provides a Part 11 Compliance evaluation including audit trails [HERE](#). Vendors of chromatography data systems, or laboratory instrument associated software can provide additional detailed information specific for their products.

If you have questions or would like additional information or assistance with GMP assessments or audits, please contact me at bwunger123@gmail.com

Unger Consulting Inc. Copyright 2014 – 2016, All Rights Reserved
APPENDIX 1

Virtually all commercially available software intended for use in the GXP regulated industries have the capability to establish audit trials. Various laboratory software may differentiate themselves by the ease of set up and user friendliness in the review process. Some software vendors have a larger family of products that are more easily networked, again, the issue of user friendliness. These features should be taken into account when making purchasing decisions.

The following questions should be considered in configuring laboratory instrument software audit trails. They are not meant to be all inclusive but provide some guiding principles to consider. Once again, it is important to remember that simply enabling an audit trail, in the absence of other necessary controls, is not adequate to ensure compliant operations.

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the firm have a policy and procedure(s) that specifies how staff are given access to computer systems?</td>
<td>The process by which access is granted, modified and removed should be governed by procedure. Job functions should govern which the systems to which individuals have access.</td>
</tr>
<tr>
<td>Does computer system access require individual log in password combinations?</td>
<td>Individual log in passwords ensure that the activity performed may be attributable to an individual. The use of shared passwords prevents this attribution.</td>
</tr>
<tr>
<td>Are actions that may be taken within the software governed by access privilege levels?</td>
<td>Actions that may be taken within the system should be controlled. Job function should govern the activities which the individual has the ability to perform. In general, those who create records should have limited or no access to significantly modify or delete records. Lists of who has which access privilege should be available for each system.</td>
</tr>
<tr>
<td>Is the date / time feature secured so that it cannot be changed by individuals who perform, supervise, review or are otherwise associated with records? Best practices include controlling the date / time feature at a network level. Consideration should be given regarding the time zone used. Some firms use the local time zone, others who may have multiple global sites who are associated with the same product may choose to use GMT.</td>
<td>A secure date / time stamp ensures that data are generated/processed/ reported contemporaneous with when the actual activity was performed. This allows the firm, reviewer, agency inspector to know WHEN an action happened. When analysts and operators can change date / time stamps it is not possible to ensure that activities were conducted at the date and time indicated.</td>
</tr>
<tr>
<td>Does the audit trail capture the identity of the individual who performed an activity within the system including logging in, acquiring data, processing and re-processing data, modifying data, reporting results, deleting data, or reviewing data.</td>
<td>The ability to capture a unique identity requires that the firm uses unique log ins and passwords. This ensures that the firm, reviewer and agency inspector know WHO performed an action.</td>
</tr>
</tbody>
</table>
Audit trails should provide the capability to document **WHY** an action was performed.

Drop down menus with prepopulated justification for actions can be problematic. They frequently lack sufficient detail to justify the action. When re-integrating chromatography data, the reason should have more granularity than simply ‘to optimize integration’. This can appear to be re-integrating until the desired result is obtained. Consider that this field in the audit trail might be a free-text field and staff should be trained to provide appropriate justifications.

**No data should be obscured or deleted** when subsequent operations are performed.

For example, when samples are retested or reprocessed including re-integration events, the original result should remain available. This ensures that all data are available for review and that **the Quality Unit considers ALL data**, including OOSs or aborted runs, **in lot disposition decisions**. If data are overwritten, deleted or otherwise obscured the Quality Unit cannot review all data records associated with an activity. Consider that the use of annotation tools may be incorrectly used to obscure problematic data in a paper print out. This is yet another reason that original electronic data should be reviewed.

Data should be reviewed in the **format in which it was generated**. Thus, most laboratory instrument data will be reviewed in an electronic format, perhaps supplemented by equipment use log books and laboratory notebooks.

Printouts of chromatograms do **not** suffice as data adequate for review, though they may be useful as a ‘convenience’ copy. GMP decisions should not be based on these printouts. Printouts, where used for ‘convenience’ often include the path to the original electronic data as a best practice.
APPENDIX 2

The eight (8) deficiencies below are taken directly from FDA warning letters that address ‘audit trails.’ These are not meant to represent all deficiencies associated with this topic, but are provided as examples of failure to meet the electronic record requirements that we’ve addressed in the first three pages. For the reader who wants to search for additional ‘audit trail’ deficiencies identified in 2015, please read the ‘warning letter’ attachment in this recent blog entry.

- ‘Because the audit trail was disabled, neither your quality unit nor your laboratory staff could demonstrate that records for these batches included complete and unaltered data.’ (Ipca Laboratories)

- ‘Your firm did not have proper controls in place to prevent the unauthorized manipulation of your laboratory’s raw electronic data. Your HPLC computer software lacked active audit trail functions to record changes to analytical methods, including information on original methodology, the identity of the person making the change, and the date of the change. In addition, your laboratory systems did not have access controls to prevent deletion or alteration of raw data. During the inspection, your analysts demonstrated that they were given inappropriate user permissions to delete HPLC data files.’ (Novacyl, Thailand)

- ‘Your HPLC software lacked an audit trail recording any changes to the data, including: previous entries, who made changes, and when changes were made. During the inspection, we also noted that all laboratory employees shared a common log-in and password to access the system. This lack of control over the integrity of your data raises questions about your analytical data’s authenticity and reliability, and about the quality of your APIs.’ (VUAB Pharma)

- ‘During the inspection, your management admitted that employees in both of your Quality Control (QC) laboratories had frequently conducted unauthorized “trial” High Performance Liquid Chromatography (HPLC) injections prior to additional injections that were used in the reported test results. Although your management stated that this practice ended in February 2014, FDA investigators discovered evidence that this practice continues. The inspection found that the names assigned to each sequenced injection were often changed during testing, obscuring the traceability of repeated injections. The data from “trial” injections was not reviewed or considered in determining batch quality.’ (Micro Labs Limited)

- ‘The audit trail for the dissolution analysis of the 9-month long-term stability sample of (b)(4) USP (b)(4) mg Tablets batch (b)(4) conducted on March 22, 2014, showed a single manual injection that was not included in the official test results package. A manual “trial” sample injection from vial position (b)(4) at 12:29 pm was injected between the Set (b)(4) and Set (b)(4) analytical sequences. No deviation was documented regarding the extra sample injection. In addition, the original injection data obtained for vial position (b)(4) was overwritten and not saved. Because the original data was
overwritten, you did not review and evaluate it as part of your batch release decision.’  
(Micro Labs Limited)

- You lacked controls to prevent the unauthorized manipulation of your laboratory’s electronic raw data. Specifically, your infrared (IR) spectrometer did not have access controls to prevent deletion or alteration of raw data. Furthermore, the computer software for this equipment lacked active audit trail functions to record changes to data, including information on original results, the identity of the person making the change, and the date of the change. Audit trails that capture such critical data about the quality of your batch production should be reviewed as part of the batch review and release process. (Yunnan Hande Bio-Tech Co. Ltd.)

- Your HPLC system had no access controls to prevent alteration or deletion of data. Furthermore, your HPLC software lacked an audit trail feature to document all activities related to the chromatographic analysis. Because of this failure, neither your quality unit nor your laboratory staff could demonstrate that HPLC records included complete and unaltered data. They were also unable to verify that there had been no alterations or deletions. (Dr. Reddys Laboratories Limited)

- Your firm failed to adequately control the use of computerized systems in the quality control laboratory. Our inspection team found that the laboratory manager had the ability to delete data from the Karl Fischer Tiamo software. During our limited review of your Karl Fischer data, we found that one file had been deleted. However, because the audit trail function for the Karl Fischer Tiamo software was not activated, and because eight different analysts share a single username and password, you were unable to demonstrate who performed each operation on this instrument system. You do not have a record of the acquisition of all data, nor do you have records of changes to or modifications of such data. (Cadila Healthcare)