Waters
THE SCIENCE OF WHAT'S POSSIBLE.®

Empower Software Audit Trails and Logs: A guide to the different locations of audit trails in Empower and what information they provide to reviewers

INTRODUCTION

Audit trails are considered the key to the security of a system since they track changes to data and metadata. In this way, an incomplete or absent audit trail can impact data integrity or even product quality. The absence of an audit trail is considered to be, "highly significant when there are data discrepancies" according to the FDA[1]

The use of computer generated, time-stamped audit trails are a significant part of the *Controls for Closed Systems. (§11.10(e)) for 21 CFR Part 11*[1] as well as regulations and guidances from across the globe, covering GMP, GLP, and GCP data.

As stated in the April 2016 *OECD Guidance Number 17 for Applications of GLP Principles to Computerized Systems*[2]: "An audit trail provides documentary evidence of activities that have affected the content or meaning of a record at a specific time point."

Additionally it has become clear that while audit trail capabilities exist on most laboratory applications, they are often not enabled, configured correctly, or part of the data review or periodic review cycle in many laboratories. Regulators are keen to see that this technical control, which enables detection of non-desirable activity by users, and provides a management tool to modify users' behavior (based on the degree of review of audit trails), is being utilized to ensure data integrity in regulated companies. Moreover, they themselves are using audit trails to review the honesty and trustworthiness of data that is being presented to them.

WHAT IS AN AUDIT TRAIL?

21 CFR Part 11 and other electronic record regulations require electronic audit trails for all data created, reviewed, modified, deleted, and archived. From Part 11, audit trails must be:

- Operator independent — no operator or administrator may change or modify in any way.
- Computer generated (automatically).
- Date and time stamped when the individual created, modified, reviewed, approved or deleted an electronic record in an unambiguous format.
- Secure — adequate security to prevent tampering.

Additionally, any change actions need to be documented automatically in the audit trail and the recorded changes must not obscure previously recorded information (i.e. record the "before" and "after" values).

Finally, the users are required to also record a scientific justification of "why" the changes are being made. This is normally documented in a comment or reason field.

- Empower® Software has the ability to discern invalid or altered records using entries in the project audit trail. Changes to methods and results automatically creates new and discrete versions of those records. This not only preserves the original but allows for comparison by highlighting differences.
- In addition, Empower provides checksum and cyclic redundancy check (CRC) verification for all human-readable and machine-readable data to protect against data being altered by external access to the system.

As highlighted in a number of the recent guidances, audit trails consist of more than simply the table you might find in an application, which is labeled "Audit Trail".

For example, in the recently updated *WHO TRS 996 Annex 05*[3] it states "Computer-generated audit trails may include discrete event logs, history files, database queries or reports or other mechanisms that display events related to the computerized system, specific electronic records or specific data contained within the record."

Conversely, certain kinds of logs, which record content unrelated to a user's creation, modification or deletion of data and may not meet the exact requirements of an official audit trail, may be misidentified as an audit trail. For instance, error logs, while useful in a troubleshooting scenario, may be simply a record of errors without the required date/time, and user details of change and justification reasons that make perfect sense in a true audit trail.

One final note — only in very critical clinical applications might you find that a user viewing a record or opening a window for read only access is actually audit trailed. In these cases no data is created, modified or deleted.

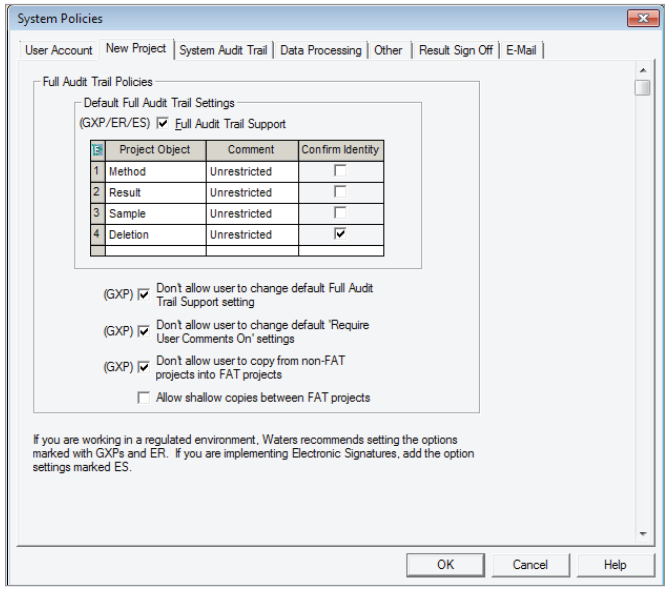
AUDIT TRAIL CONFIGURATION

Audit trails should be enabled prior to any regulated data being collected in an application. While this could be set by default, it might be configured by the vendor upon installation or it may be configured by the administrators at the regulated company.

Software applications may allow both regulated and non-regulated users to work in the same application but with different audit trail settings for their specific projects. In this kind of configuration, care should be taken to ensure that these working practices are segregated and managed such that regulatory data cannot be created, modified, or deleted in non-regulated/non-audit trailed areas.

OECD Guidance Number 17[2] states quite clearly that "The ability to make modifications to the audit trail settings should be restricted to authorized personnel." Additionally audit trail configuration changes should themselves be fully audit trailed.

Empower audit trail settings can never be modified once a project is created. The Empower policies only affect the options available for new projects. While vendors may make suggestions about settings such as audit trail configuration, an individual regulated company may be using the application in a unique way, either alone or in conjunction with other computerized or paper based systems. It is therefore important for settings to be adjusted to reflect the intended use and acceptable risk of any laboratory.



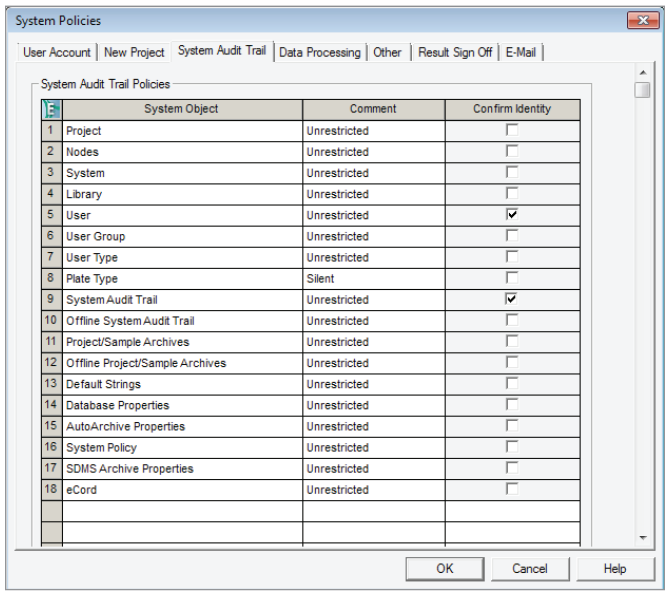


Figure 1 and 2. The New Project and System Audit Trail Policies for Empower can be set by privileged users according to the intended use and acceptable risk of the laboratory.

AUDIT TRAIL TIME STAMPS

Time stamps for record creation as well as audit trails need to be standardized and consistent. It is critical that time sources are synchronized and protected from alteration by users, managers and even administrators. It is common that time stamps are taken from the time of the operating system and, particularly in standalone systems (single computer PC's), this level of protection may be difficult to control. However, in network deployments, it is much easier to synchronize and control access to time sources.

For standalone or site-wide solutions, local time may be preferred. When wider, cross time zone installations are deployed, consideration of UTC or a fixed timezone may be needed, if managing users and instruments in multiple time zones is unobtainable.

- Empower Enterprise solutions allow specific time zones to be specified for acquisition clients, processing clients, Citrix clients and servers.

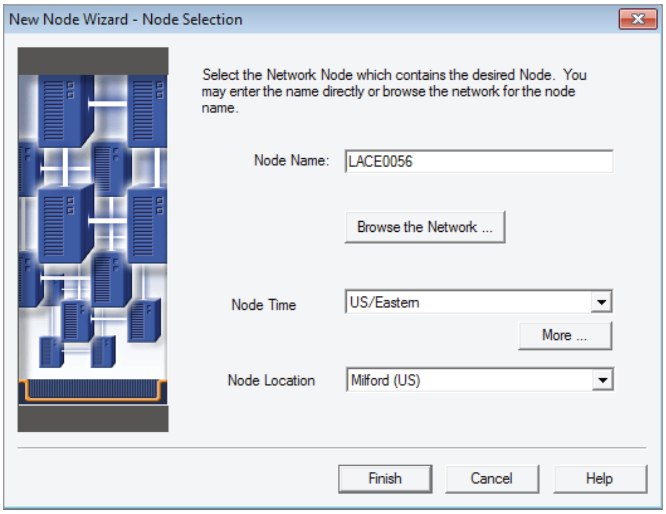
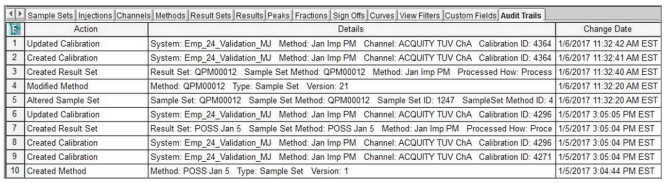


Figure 3. During creation of a Node connection in Empower, the Node time zone and Node location can be set.

A good understanding about how any specific application leverages time stamps (and additional controls put in place in the IT infrastructure), help with confidence in the correct sequencing of actions noted in the audit trails, referred to as "operational system checks to enforce permitted sequencing of steps and events" as stated in *§11.10(f) for 21 CFR Part 11*.[1]



	Action	Details	Change Date
1	Updated Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4364	1/6/2017 11:32:42 AM EST
2	Created Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4364	1/6/2017 11:32:41 AM EST
3	Created Result Set	Result Set: QPM00012 Sample Set Method: QPM00012 Method: Jan Imp PM Processed How: Process	1/6/2017 11:32:40 AM EST
4	Modified Method	Method: QPM00012 Type: Sample Set Version: 21	1/6/2017 11:32:20 AM EST
5	Altered Sample Set	Sample Set: QPM00012 Sample Set Method: QPM00012 Sample Set ID: 1247 SampleSet Method ID: 4	1/6/2017 11:32:20 AM EST
6	Updated Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4296	1/5/2017 3:05:05 PM EST
7	Created Result Set	Result Set: POSS Jan 5 Sample Set Method: POSS Jan 5 Method: Jan Imp PM Processed How: Proce	1/5/2017 3:05:04 PM EST
8	Created Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4296	1/5/2017 3:05:04 PM EST
9	Created Calibration	System: Emp_24_Validation_MJ Method: Jan Imp PM Channel: ACQUITY TUV ChA Calibration ID: 4271	1/5/2017 3:05:04 PM EST
10	Created Method	Method: POSS Jan 5 Type: Sample Set Version: 1	1/5/2017 3:04:44 PM EST

Figure 4. An Empower project audit trail showing the time zone included in the time stamp.

AUDIT TRAIL REASONS FOR CHANGE

One critical aspect of audit trails is the documentation of the reason "why" an action was performed. This level of detail is almost never possible to be populated by the software application automatically as it requires the input of the user performing that action. Free form reasons allow the user to truly express why an action was performed, while pre-defined reasons are available for noting common reasons.

- Empower offers users silent, pre-defined or free form use of reasons to document why an action has been performed.
- View Filters in Audit Trails allow reviewers to search for specific data, specific actions, or specific reasons for actions.

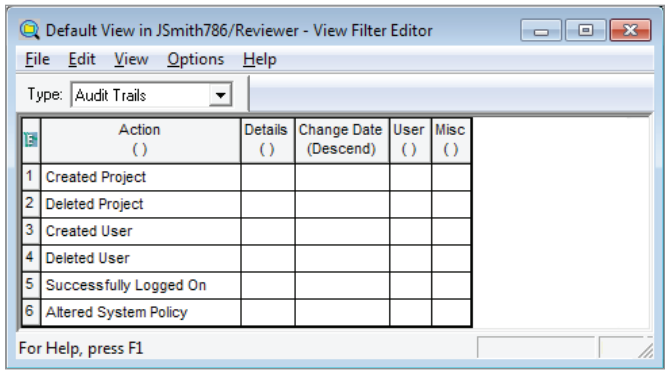


Figure 5. View Filters on Audit Trails can be created to search for specific data; specific users, specific actions, or specific reasons for actions.

ENSURING THE AVAILABILITY OF AUDIT TRAILS

The audit trail documentation must be retained for the same period as the electronic record. Accurate and complete copies must be made available to the auditor (whether internal or external) for review and copying, and must be both human-readable and machine-readable.

- All records, histories, and audit trails are automatically backed up during security back up routines of Empower.
- Empower Audit Trails at the project level and below are always archived and restored when the project is archived or restored, ensuring that any metadata relating to a specific analytical result cannot be lost during the record lifecycle.
- System Audit Trails may be archived to a secure format, readable only in the Empower application, or exported in a converted, non-secure format.
- Archiving the System Audit Trail, like other archiving activities, may be a manual process, or with the use of NuGenesis LMS, this task may be automated.

EMPOWER SYSTEM AUDIT TRAIL

- Empower 3 Software System Audit Trail provides a history of actions that affects the overall system configuration (such as denied login, project archival, changes to system policies etc.).
- 'System' here refers to the overall Empower application and should not be confused with an analytical instrument system or HPLC system audit trail.
- Changes to user privileges are tracked.
- All system-level actions in Empower, even those performed by administrators, are recorded.
- Audit trails are generated automatically and cannot be modified.

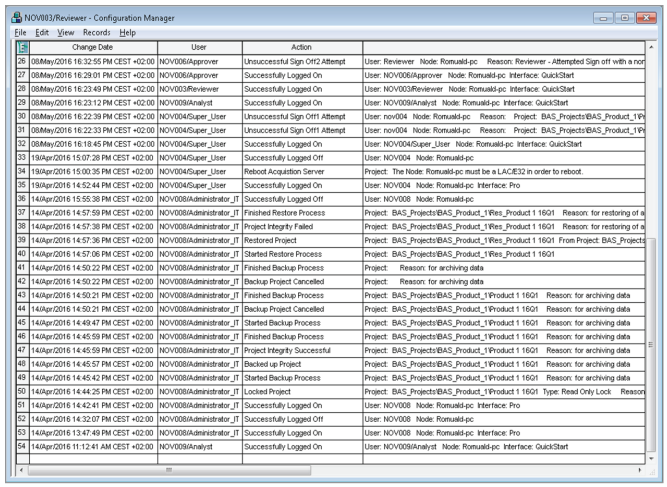


Figure 6. Readable view of the Empower System Audit Trail which can be filtered and sorted to find and print relevant records.

EMPOWER PROJECT AUDIT TRAIL

- The Empower Project Audit Trail is an overview of every activity performed by users, as well as data, metadata, and methods inside that project.
- The Project Audit Trail captures information that affects the data within a project (sample set information, calibration curves, method changes, processing data) and other information captured in the Empower database (who, when, what, and why) including any data creation, modifications to metadata, record copying, deletions and signature actions.
- Further details can be found in individual item histories such as Acquisition or Injection Logs, Method Audit Trails, Sample or Sample Set Histories.

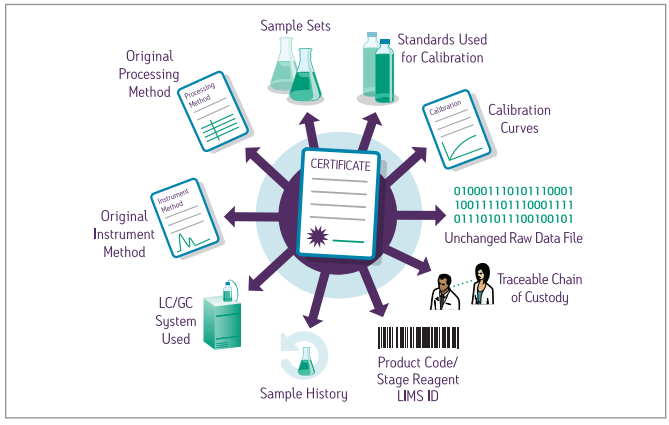


Figure 7. The Oracle database underlying Empower, creates permanent linking relations between methods, dynamic electronic data, and metadata which cannot be broken, permitting easy query and review of related data.

ACQUISITION AND INJECTION LOGS

Integrity of data during a chromatographic run may also be important. Although there is a record of the instrument parameters, could there be a way for an analyst to make "alterations on the fly" or influence the run in other ways, before the data is securely saved?

Most chromatography data system (CDS) solutions and instruments have a number of technical controls to prevent altering data, such as locking front panels or recording interactive changes.

- Empower permanently stores the exact instrument method that was used to collect the data with any chromatogram.
- If a system allows interactive changes (through either an unlocked front panel, separate controller, or console software) and users have permissions to perform interactive changes during a run, those changes are recorded in an Acquisition Log which is permanently linked to the raw data.
- For some specific Empower-controlled instruments there may additionally be a Post Run Report to verify the actual acquisition settings or experimental conditions for e.g. MS data acquisition.
- The Acquisition and Injection Logs are viewable in older Empower versions though a special report group in Report Publisher.
- Since Empower 3 FR2, Acquisition Logs are displayed with other audit trails in the Result History tab within the Result Audit Viewer.

METHOD HISTORIES

- All methods in Empower are never overwritten and are automatically versioned.
- Methods are assigned unique ID's (within the project) upon creation, with all previous versions available for review, and permanently linked to any results that were generated using them.
- Methods can be locked, assuring that modifications can never be made.
- While an indication of changes to any Empower method exists in the project audit trail, more details of the change are additionally stored in each method properties.
- Method properties shows the history and all versions of the method, including the reason for change.
- Older versions of methods can be "made current" allowing users, if permitted, to restore an earlier version into use.

COMPARE METHODS

While audit trails provide a history of modifications made to a method, often it may be required to compare two different methods or two versions of the same method to view the details of the change, including the 'before and after' values. This could be useful to determine if all changes adhere to any standard operating procedure (SOP)-mandated allowable changes.

- Empower's Compare Methods feature may be used to compare two methods with different names or two versions (either historical or current) of the same method.
- Compare Methods feature can be used for instrument methods, sample set methods, sample set method templates, method sets, processing methods, report methods and export methods.
- Method comparison tables may be searched to look for key parameter alterations.
- Documenting and reviewing method ID's, limiting permissions to change methods, or locking methods may negate the need to examine method histories in detail, as method changes would be easily observed, restricted or prohibited.

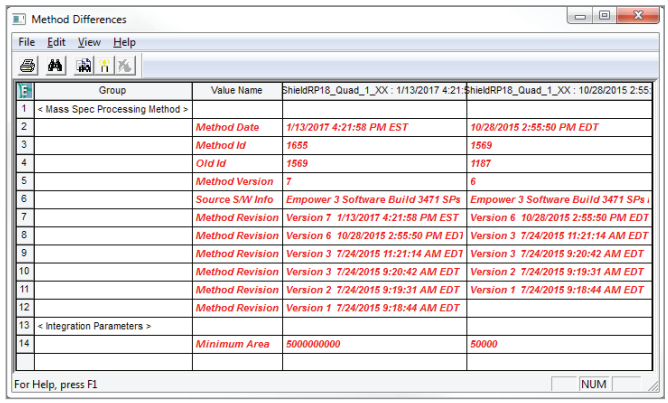


Figure 8. Difference between methods and method versions, as used in Empower can easily be shown and differences highlighted.

SAMPLE AND SAMPLE SET HISTORIES

Changes to sample metadata are often required. Metadata may be as simple as a sample name or text field but may also be a critical value that is required to calculate the final results. Modification of metadata may be needed, either pre or post-run, to complete missing metadata or to correct incorrectly entered metadata.

Metadata changes will often be simple corrections or may indicate an attempt to influence the final results.

Changes to sample metadata should therefore be audit trailed, with the 'before' and 'after' values recorded automatically so that previous values are not obscured and are associated with an acceptable justification.

Records where metadata has been altered should be flagged, indicating that a deeper review is needed as part of a risk-based quality management system.

- Changes to sample metadata are performed using the Run Samples window or the Alter Sample tool.
- Raw data and records, where the sample metadata has been altered, are permanently flagged.
- Existing results, generated with the original data, remain unchanged and data must be processed using the new values, creating new and distinct results.
- Sample metadata changes are audit trailed in Empower through both the Project Audit Trail and Sample and Sample Set Histories.
- Sample and Sample Set Histories are traditionally viewed from the Altered Sample tool, but may also be seen in the new Result Audit Viewer. Sample and Sample Set Histories display the original and new values as well as the user, time and reason for change.
- Sample and Sample Set histories may be included in Reports. However, the level of required detail could fill dozens of pages for a single run, and therefore a review is more typically performed on the original electronic record using the Empower application, under a risk-based approach based on the altered flag and other indicators.

REVIEWING AUDIT TRAILS

New requirements of European regulations (*GMP Annex 11*) to regularly review audit trails are also being expected by FDA investigators. Even though there is no formal mention of this in Part 11, companies that fail to have a formal process to review audit trails have had this omission cited in official observations or warning letters.

Most regulated companies treat audit trails relating directly to data and results as an integral part of the metadata needing to be reviewed based on a risk-based approach before batch or study release. This may follow a "review by exception" approach, as is typically performed for other metadata.

- Empower can assist in meeting this expectation by providing easy access to method, data, results, and metadata audit trails from the Review screen. This capability is available in all versions of Empower Software.
- A new tool introduced in Empower 3 FR2, called the Result Audit Viewer, brings together audit records from the Project Audit Trail, Acquisition Log, Method, and Sample Histories into a single window, and also permits easy comparison of methods and results.

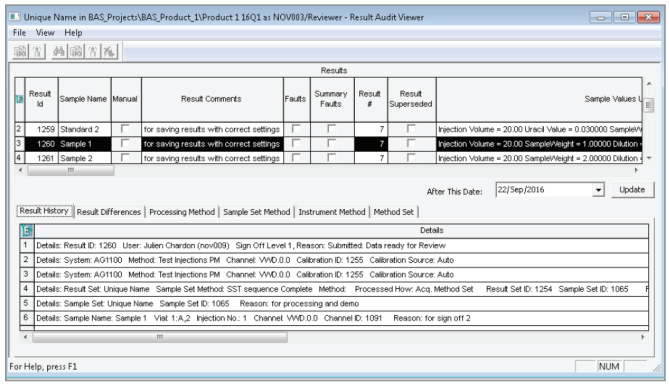


Figure 9. The Review window and the new Result Audit Viewer facilitate a reviewer to interrogate the data, methods, peak results, calibration curves, and audit records, and then take the results directly to Preview for electronic sign-off.

Managing and reviewing the System Audit Trail is typically performed as part of a regulated company's periodic review process, which many local regulators require for computerized laboratory systems e.g. *PIC/S GMP Annex 11*:

- Empower System Audit Trail provides View Filters to search for specific events which may indicate improper use of the system at the administration level.
- Specific views can be created to display only the information needed for review. Additionally, ad hoc views may be created to, for example, search for all actions by a specific user.

INCLUDING AUDIT RECORDS, LOGS, AND HISTORIES IN REPORTS

In a hybrid laboratory that has yet to fully embrace electronic data review and still largely relies on paper records, the requirement to now include audit trail review can present a major obstacle. Many of the new guidances clearly define reports as "static" records that do not preserve the "dynamic" nature of the original electronic record which permits a more forensic review of laboratory (e.g. integration baselines.)

Additionally, while regulators are requiring review of significantly more metadata, such that a review must include the "complete" data, the challenge of presenting all the available dynamic electronic data on a static paper or PDF report becomes insurmountable.

As well as audit trails, regulators may include in their definition of "complete data" every chromatographic run of a specific sample, (even those rejected because of a failed system, injection, column or solvents), every version of a result, (potentially even those rejected because of poor or inaccurate integration or incorrect metadata), and all versions of sample sets and methods.

The FDA themselves do not believe that, for anything more complicated than a simple balance or pH meter, any static report can be defined as a true and complete copy of the original electronic record. Review of the original and complete electronic record is expected.[6]

- "The printed chromatograms used in drug manufacturing and testing do not satisfy the predicate rule requirements in 21 CFR Part 211."[7]
- "The electronic record must be maintained and readily available for review by, for example, QC/QA personnel or the FDA investigator."

The *WHO Guidance,*[3] however, does propose a way to create and leverage paper or PDF summary reports for further decision making:

- "Paper printouts of original electronic records from computerized systems may be useful as summary reports … verify that the printed summary is representative of all (electronic) results."
  - Note that this can only be done after verification that the summary is trustworthy and all-inclusive.
- "Data integrity risks may occur when persons choose to rely solely on paper printouts or PDF reports."
- "If the reviewer only reviews the subset of data provided as a printout or PDF, these risks may go undetected."

While many laboratories still continue to create paper copies of electronic records in the form of reports and rely on these to review them, the task of now creating giant reports, including audit trails, and the risk that critical notifications may be lost in the sea of printed data, pose a significant risk to product quality and data integrity. This specific risk is also mentioned in the *WHO Guidance*.[3]

DOCUMENTING DATA REVIEW INCLUDING AUDIT TRAIL REVIEW

Documentation of audit trail review should be performed in a similar way to documentation of any review process. Typically this is done by signing the results as 'reviewed' or 'approved', following a data review SOP which outlines how the review process should be performed, and will include how and when to review audit trails.

The *WHO Guidance*[3], notes that under the section for documentation of data review on paper records, a signature is added to the actual records reviewed, while, in the "expectations for electronic records" you follow a clear procedure and then electronically sign the electronic data set as having been reviewed and approved.

Thus it would seem unreasonable to require specific 'evidence' of exactly which records and metadata were looked at or opened. This might be considered an audit trail of the review process, or an audit trail of the audit trail review process. Perhaps keystroke tracking or video recordings may be the only way to achieve this electronically.

Other non-audit trail logs

In addition to the audit records detailed above, there are other logs and messages regarding the Empower application, instrument drivers, and the host operating system available to the user which do not meet the definition of an audit trail. These include, but are not limited to the Windows Event Viewer, Empower Message Center, and pop-up messages from Empower or any other application. Like most kinds or error logs or histories, these logs may not always be permanently retained, as their usefulness is time dependent.

The Empower Message Center is an interface that brings together pertinent informational, warning, and error messages generated by Empower applications, which might otherwise only display in a pop up message. These messages may be from Waters or third party instruments and drivers, third party applications via the API toolkit, as well as from pieces of Empower code.

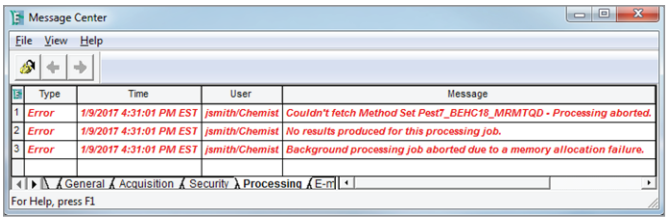


Figure 10. The Empower Message Center displays error messages from instruments, third party applications, and Empower Software for troubleshooting purposes.

For quick reference, the Message Center typically displays only the messages relating to the currently logged in user. Error messages relating to all users in the system will be displayed if the current user has appropriate privileges.

The Message Center is not intended as a replacement for, or a component of, the audit trail. Any critical messages related to the users' creation, modification, or deletion of data are always permanently saved into the associated audit trail or acquisition log along with the users' justification when appropriate. Message Center messages more often than not describe some requested action which could not be completed.

Due to the high volume of messages collected in the message center in large deployments of Empower, the Message Center was designed with functionality to remove messages. Either a manually instigated or a time-based auto-purge (where the user specifies the time) may be utilized. Not proactively managing the size (history) of the message center will adversely affect system performance where there are many active instruments.

Laboratories may have a desire to export and retain copies of these messages in external files or systems for troubleshooting purposes. Neither purging nor exporting messages will affect the availability of audit records related to them, which are permanently stored in the relevant audit trails.

Within the overall Empower application, instrument control consoles may also include their own cache of error logs. For instance, the ACQUITY® PDA Detector has its own log tab in its console.

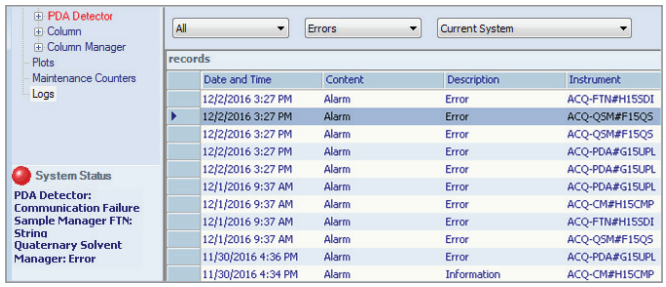


Figure 11. Additional Logs may exist in specific instrument console pages.

The Message Center and other available logs and messages are intended to aid in user level monitoring and/or troubleshooting in the laboratory; either independently or with the assistance of Waters' or third party technical support.

SUMMARY

Empower Software provides tools to capture users actions as they relate to data creation, modification, and deletion. The unique way Empower utilizes the Oracle database ensures that the links between various records can never be broken, including the links between audit trails and results or methods.

Reviewing audit trails makes the most sense as an integrated part of the data review process, so it is essential that the reviewers have a good knowledge of how Empower Audit Trails are designed and work together with the data. The extent of audit trail review should be considered, along with the extent of any other critical metadata which should be included in peer review and approval review. A clear SOP to identify the frequency, roles, responsibilities, and approach to a risk-based review of data and metadata including audit trails (as well as documentation that this is adhered to) should be developed and followed. Periodic review processes should investigate the effectiveness of the data review SOP.

References

1. FDA Title 21 chapter 1 Subchapter A Part 11 (21 CFR Part 11) Electronic Records; Electronic Signatures from www.ecfr.gov
2. ENV/JM/MONO(2016)13..... OECD Series Number 17: Application of GLP Principles to Computerised Systems 22-APR-2016 available on http://www.oecd.org
3. WHO_TRS_996 Annex05 http://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf
4. EudraLex Volume 4 GMP Medicinal Products for Human and Veterinary Use; EU GMP Annex 11 Available from: http://ec.europa.eu/health//sites/health/files/files/eudralex/vol-4/annex11_01-2011_en.pdf
5. PIC/s GMP Guide (PE 009-13 (Annexes) Annex 11: Computerised Systems Available from https://www.picscheme.org
6. Questions and Answers on Current Good Manufacturing Practices, Good Guidance Practices, Level 2 Guidance - Records and Reports; Available from: http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124787.htm
7. FDA Title 21 chapter 1 Subchapter A Part 211 (21 CFR Part 211) GMP for Finished Pharmaceuticals from www.ecfr.gov

Waters

THE SCIENCE OF WHAT'S POSSIBLE.®

Waters Corporation
34 Maple Street
Milford, MA 01757 U.S.A.
T: 1 508 478 2000
F: 1 508 872 1990
www.waters.com