Audit Trails in Lab Environments – Overview and Best Practices

Audit trails are an essential component of regulatory compliance in the pharmaceutical sector. They are also crucial for ensuring patient safety as well as delivering a range of other benefits. There are two main types of audit trails that apply to pharmaceutical laboratories – system audit trails and data audit trails.

While they are both different, the principles and best practices of system audit trails and data audit trails are essentially the same.

Differences Between System Audit Trails and Data Audit Trails

System Audit Trails

System audit trails apply to systems in your lab, such as software applications, so they are focused on system settings and actions. With system audit trails, all system-level actions performed by the administrator should be automatically captured, including user administration, security settings, permissions, etc. System audit trails need to be validated, and review processes should be based on risk, where data that is critical to patient safety and/or regulatory compliance is identified for periodic review.

Data Audit Trails

Data audit trails, on the other hand, apply to data and results. An example is the data produced by a high-performance liquid chromatography (HPLC) instrument. There needs to be an audit trail of this data, with the audit trail subject to regular review in a process often referred to as a Second Person Review. These reviews are required for compliance, but they are also typically part of study or batch release quality control processes.

What Are Audit Trails?

Audit trails should cover the creation, modification, and deletion of all data that is produced in a lab environment, as well as all system-level actions. For example, a data audit trail should include who worked on a sample, the time and date of the work, the work that was done, and why the work was done. The original data should be retained as well as the changed data as a result of the work.

Furthermore, audit trails should comply with data integrity standards. This means putting in place processes, practices, and systems that prevent the data from being edited, lost, or obscured. It is also important that data in audit trails is searchable.

We can also look at regulatory guidance and definitions to get a deeper understanding of audit trails, what they are, and why they are important. For example, FDA guidance on data integrity says an audit trail is 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".

The FDA guidance quoted above uses the example of an HPLC run. In this example situation, the audit trail should include the run's date and time, as well as user details, integration parameters, reprocessing details, and reprocessing change justification information.

We can also look at 21 CFR Part 11 which has a similar description of audit trails. It says:

> "Use of secure, computer-generated, time-stamped 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. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying."

Benefits of Robust and Reliable Audit Trails

- Improves the safety, quality, and efficacy of pharmaceutical products.
- Ensures accountability.
- Helps prove compliance with regulations.
- Helps diagnose and correct problems with processes.
- Helps identify suspicious activity.
- Helps to prevent fraud.
- Enables process optimisation as audit trails can be used to identify fluctuations from the normal baseline, as well as process bottlenecks and performance improvement opportunities.

Best Practices

The first point to highlight is that generally applied standards for audit trails are not sufficient for the pharmaceutical industry or pharma labs. For example, a cGMP-compliant audit trail will store data in a relational database management system (RDBMS) where libraries can be created, the data's event log can be queried, etc. This is not a standard requirement for audit trails in other industries.

So, it's important to make sure systems, software applications, and processes have audit trails that meet the regulatory and patient safety requirements of the pharmaceutical industry.

It is also important to automate the process as much as possible. Automating the creation, updating, and maintenance of audit trails and audit trail data significantly reduces the risk of human error. The goal should be to minimise human involvement as much as possible.

Other key best practice principles of audit trails include:

- Secure – audit trails should be stored securely, and users should not be able to edit them.
- Contemporaneous – audit trail data should be recorded at the time of the event rather than at a later date or time.
- Traceable – audit trail data should be attributable, updates should not obscure previous values, and reasons for changes should be recorded.
- Archived – audit trail data should be stored for as long as required.
- Available – audit trails should be searchable and there should be the ability to run reports.

We can also look to cGMP best practices and minimum requirements to ensure system audit trail data integrity:

- Data recorded in audit trails should be complete.
- Complete and accurate backups of audit trails should be taken at regular intervals. Backups should also be properly secured to ensure they can't be altered or lost, either deliberately or inadvertently.
- The storage of audit trails and audit trail backups should ensure there is no deterioration of data over time.
- Systems creating audit trail data should be properly calibrated and checked for accuracy.
- Reproductions of audit trails should be accurate and complete.
- Lab processes and controls should be reviewed and verified.

Importance of Periodic Audit Trail Reviews

In modern, increasingly digitalised pharmaceutical labs, effective and efficient compliance with audit trail guidance and regulations requires technical solutions. These solutions need to be properly set up and configured but it is equally important to conduct regular security

and audit trail reviews. Reviews will identify problems in your processes and electronic records so they can be returned to a compliance state.

At Westbourne IT, we have technical expertise as well as pharmaceutical industry and regulatory knowledge and experience. This means our team can help with your periodic security and audit trail review requirements, in addition to IT compliance audits and validation services. Get in touch today to speak to a member of our team.