http://www.contractpharma.com/issues/2014-09-01/view_features/the-audit-trail-advantage/

# The Audit Trail Advantage

**Why one of FDA's most misunderstood rules can help ensure data integrity and compliance, and help in root cause analysis**

By Carol Brandt , GMP Compliance Consulting, NNE Pharmaplan
Published September 8, 2014

The audit trail is an integral requirement of an electronic record, ensuring the validity and integrity of the record and the link between any electronic signature and the record associated with it. Its regulatory requirements are fairly straightforward, but the benefits it offers are often misunderstood.

Audit trail reports can be reviewed to identify system security issues, errors in sequencing of activities, investigation of errors and unexpected events, training issues, and data integrity events. They can also add supportive evidence to a contract vendor audit.
Audit trail report reviews can significantly benefit the regulated environment manufacturer, providing detailed accounts of the activities performed on a computer and the status of the electronic records.

Before computers were commonly used in the regulated environment, paper records universally documented the activities and events, as they happened, time/date and by whom. In the event that a change is made to the record, Good Documentation Practices (GDP) require that the initial entry be lined out but not obscured, the change entered, signed, dated and in some cases a reason for the change is also documented. The act of storing or saving data/information to media (including disks, flash drives, floppies, and CD's) constitutes creation of an electronic record, which in the early 1990's, were unregulated and subject to uncontrolled manipulation.

In 1991, the pharmaceutical industry requested that the FDA define the requirements by which paperless systems could be used under the current cGMPs (Good Manufacturing Practices). With the introduction of the routine use of computers in the regulated industry, the Regulatory Agencies became aware that it was possible to create, modify and delete data without the same controls required of paper records. These issues, along with the industry requests, spurred an Agency task force in 1992 and the publication of the final rule to control electronic records, 21 CFR (Code of Federal Regulations) Part 11, "Electronic Records; Electronic Signatures" (Part 11) in 1997.[1,2]

## Industry was Unprepared for Part 11

Response from the industry was that additional time was needed to be able to comply with the ruling, and the FDA (Food and Drug Administration) delayed its enforcement until 1999. Many pharmaceutical manufacturers were unprepared, and rushed to try to understand Part 11 and assess their computers and compliance, by preparing Part 11 Site Plans and executing remediation activities.

One of the major issues at that time was that the software vendors hadn't planned for the ruling either, and although basic security features were built into many software packages, audit trails were not, or if they were, they were not fully compliant with the requirements. Even many of the software vendors provided limited security options such as one User Name/Password for anyone operating the system. "Legacy systems" were defined by the FDA as those in effect before 1997, and were initially exempt from the ruling. However, if changes were made to the systems after the ruling became effective in 1997, those systems were subject to compliance with Part 11. "Certain older electronic systems may not have been in full compliance with Part 11 by August 1997 and modification to these so called "legacy systems" may take more time. Part 11 does not grandfather legacy systems and FDA expects that firms using legacy systems are taking steps to achieve full compliance with Part 11."[3]

Besides regulations around the use of the audit trail in electronic records, Part 11 details requirements for the electronic signature, and validation of the computer system. The industry had a difference of opinion on how to deal most effectively with Part 11; some took a risk-based approach and tried to comply with their Site Remediation Plan over time; where they could, others discontinued the use of electronic signatures and records, and reverted to a paper solution.

The operational benefit of validating computer systems has been realized and accepted by the industry, however, general fear of the regulation and how to comply still exists in the pharmaceutical industry today, because the audit trail requirements are largely misunderstood. Even to date, there are numerous firms that are unable to readily print audit trails from their GMP computer systems and have never looked at the audit trail reports.

## Audit Trail Requirements

"Audit Trail means…a secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record."[4]
FDA's "Guidance for Industry—Computerized Systems Used in Clinical Trials,"[4] summarizes the audit trail requirements:

1. "Section 21 CFR 11.10(e) requires persons who use electronic record systems to maintain an audit trail as one of the procedures to protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records.

a. Persons must use 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. A record is created when it is saved to durable media, as described under "commit" in Section II, Definitions.

b. Audit trails must be retained for a period at least as long as that required for the subject electronic records (e.g., the study data and records to which they pertain) and must be available for agency review and copying.

2.Personnel who create, modify, or delete electronic records should not be able to modify the audit trails.

3.Clinical investigators should retain either the original or a certified copy of audit trails.

4. FDA personnel should be able to read audit trails both at the study site and at any other location where associated electronic study records are maintained.

5. Audit trails should be created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data in violation of §11.10(e)."[4]

Title 21 CFR Part 11, Subpart B "Electronic Records", §11.10 (e) Controls for Closed Systems, describes the requirements for the audit trail as follows:

"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."[1]

Therefore, the audit trail applies not only to events recorded in the electronic record, but events associated with electronic signatures that are applied to the electronic record in the appropriate sequence (review, approval, signature, time/date). This is no different than the paper record requirements described in the History Section above. Changes, deletions, signatures and time/date stamps are applied securely to the electronic record just as they would be to the paper record, which is the purpose of the audit trail.

## Audit Trail Use and Benefits

Software vendors supplying packages to the regulated industry are, for the most part, now providing Part 11 "compliance capable" software. This means the system contains the code to make the software configurable to be Part 11 compliant, not that it's automatically compliant. For instance, the basic "off the shelf" software has to be configured for certain end-user security access level requirements and to require electronic signatures based on the function. If system access isn't limited by design, i.e. the manner in which the user configures it, and the User ID and password aren't both unique to the individual, the system is not compliant.

For some more complex systems, such as ERP (Enterprise Resource Planning) systems that manage finances, warehousing, product release, etc., the audit trail can be enabled or disabled for individual transactions (functions) and associated data tables, by customizing the software configuration. If the audit trail is disabled for any GMP functions or for a function requiring electronic signatures (such as product release), the system is not Part 11 compliant.

The audit trail can provide important information to the pharmaceutical firm to track system access, what activity occurred, sequence of events, by whom, and by when. (For a flow chart showing a typical audit trail, see Figure 2).

## Ensuring Data Integrity

Data integrity is the foundation of regulatory compliance, and often found lacking in FDA 483's

and Warning Letters. However, it can be established by the history in the audit trail. Firms that have implemented a routine review of audit trail reports benefit from having evidence that procedures are being followed and data integrity confirmed.

For computer systems capable of producing an audit trail report (also required by Part 11), a routine review of the report can identify security, training and integrity issues immediately. For example, Figure 1 is an example of a lab audit trail report which identifies several flaws in the analysis performed.

Potential issues with the assay are:

1. Logon doesn't identify the user by name, indicating there is a group logon being used;
2. Standard 1, vial 1 was injected twice;
3. Two vials of standard 1 were injected while only 1 vial of standard 2 was injected;
4. The third injection of the 40/75% stability sample was deleted indicating that data deletion is possible. It also indicates the Analyst has access rights, which could potentially allow for the deletion of data.

## Audit Trail Review

A periodic review of audit trail reports should be performed on each computer system generating GMP data that could impact product safety, purity and efficacy. Focusing the review on the more critical computer systems based on a documented risk assessment of the data produced, is a way to minimize the workload of the task. A monthly routine audit trail review should be implemented for critical GMP systems and functions, or within days if required to investigate an error, security breech or other deviation.

Some of the more complex computer systems generate volumes of audit trails, so it is beneficial to apply a documented risk assessment to the more critical functions of the computer, to identify the highest risk audit trail reports to review. Consideration at highest risk compliance should be given to systems that require an electronic signature to meet predicate rule requirements (electronic batch records, etc.) and critical functions of system that might include product disposition (release, reject).

The review should be detailed in a written procedure and signed/dated by the reviewer. The audit trail may also be supported by and should be checked against cross-referenced information in a lab notebook and/or documented lab events/investigations.

## Contract Vendor Audits

The audit trail report of any computer system with a high compliance risk to GMP data used to support product claims can provide a rapid initial assessment of the integrity of the electronic records. The review should always be included in a contract vendor (manufacturing or laboratory) audit.

Laboratory data records are particularly vulnerable to manipulation and unauthorized access, including inappropriate access levels. Although the audit trail review in itself doesn't constitute a data integrity audit, it can provide early warning signs, even of a basic security breech or

inappropriate access rights (for instance, approval of one's own work).

## Beyond the Audit Trail

As stated above, the review of an audit trail report may not in all cases be used independently to conclude electronic record integrity. Assuming the audit trail of data collected from equipment indicates no data manipulation, security or sequential issues are noted, the electronic data files that are collected from laboratory equipment, for example, may be stored locally on that computer, and could be unprotected from manipulation. It's therefore important to identify system connections to other computers and storage devices.

Unless the files are locked when they are stored, data can be manipulated after it is collected, and resaved under the same file name. Real-time storage of data to secured servers is the only way to assure data is protected once it's stored.

Uploading of data to other software, such as Excel spreadsheets, for example, may generate additional electronic records which also require limited access and protection from changes. Audit trails are not generated in the typical use of Excel spreadsheets, so data should be protected through security and locked cells and files.

In short, security access, data integrity, sequencing of events and activity detail can readily be reviewed in an electronic audit trail report which, compliant with 21 CFR Part 11, details every action that occurred from the point of system logon to logoff. This allows for the identification of unauthorized changes or deletion of data, alteration or deletion of files, and process/procedures not being followed, with the intent to ensure electronic records are trustworthy and reliable.

---

**Carol Brandt** has over 30 years of experience in the Pharmaceutical industry as a professional with expertise in strategic insight and extensive knowledge of Quality Assurance and Computer Compliance in the healthcare industry. For several global pharmaceutical and biological sciences companies, Ms. Brandt has managed systems operations across a global organization, supporting regulated quality assurance operations, diagnostic computer system groups, electronic record systems, manufacturing and production systems. She has held VP positions in the life sciences industry in Quality Assurance operations as well as FDA-related information technology validation roles. Her responsibilities have included site licensure, FDA inspections, inspection preparation, Regulatory responses and compliance with pharmaceutical State, local, FDA, CBER, CLIA and European regulations in compliance 21 CFR Parts 210, 211, 111, 820 and 11. She has also been responsible for compliance development of Quality Systems, processes, policies and procedures for OTC, dietary supplement, pharmaceutical and medical device industry leaders firms.

**References**

1. Code of Federal Regulations, Title 21 Food and Drugs (Government Printing Office, Washington, DC), Part 11, 62 FR 13464, Mar. 20, 1997.
2. S. Naeymirad, Electronic Records, 21 CFR Part 11 and Oracle 9i, internet presentation.

3. FDA, “Inspections, Compliance, Enforcement, and Criminal Investigations, Attachment A Computerized Systems”, (May 6, 2009).
4. FDA, “Guidance for Industry – Computerized Systems Used in Clinical Trials”, (Apr, 1999).