An Executive Summary

Does Your Electronic Data System Meet 21 *CFR* Part 11 and CGMP Requirements?

Know and understand your electronic data system and workflow.

Humera Khaja
Global Software Compliance Program Manager
Agilent

Introduction

For laboratories that need to meet the regulations of 21 *CFR* Part 11 and CGMP, there must be procedures in place for data integrity. Key to this is understanding where and how data systems log information throughout the data lifecycle: from data generation, through reporting, review, and archival.

This paper explores the critical areas that need to be explored and verified for data integrity in each step of the analytical workflow—from understanding the key aspects of an e-workflow in relation to business processes, to discovering what technical controls exist inside software and how they affect data integrity.

FDA's Definition of a Closed System

FDA defines a closed system as "an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system" (21 *CFR* Part 11.10 and Part 211.194).

The rule further states that a person who uses a closed system to create, modify, maintain, and transmit electronic records should employ procedures and controls designed to ensure the authenticity of electronic records and to ensure signatures cannot be repudiated. The regulation of closed systems includes, but is not limited to: procedures and controls such as validation of systems, protection of records, limiting system access to authorized individuals, existence and use of audit trails, and the use of operational system checks.

In addition to the regulation of closed instrument data systems, the laboratory environment must also satisfy CGMP requirements. An example is any production or laboratory control

SPONSORED BY
Agilent OpenLab

LC|GC north america

record that must be reviewed for accuracy, completeness, and compliance with established standards that satisfy the Parts 211.22.192 and 194.

Do You Really Know Your Electronic Data System?

Data systems need front and back end controls. Front-end controls ensure data are collected by specific trained users such as technicians or laboratory scientists per established SOPs. Such controls include:

- Permission control ensuring the appropriate users have the right to access and perform certain steps in the workflow.
- Version control for all data sets and templates ensures traceability.
- Electronic signatures are used properly to review and approve and have relevant metadata for completeness and context.
- Audit trails and activity logs are reviewed providing context to help “recreate” the story of the data set, along with the instrument parameters for any given timeframe.

Back-end controls handle data collection. Once the data are collected, they must be stored and managed appropriately to satisfy regulation 11.10 (a) the ability to discern invalid or altered records, (b) generate accurate and complete copies of the records for inspection, review, and for copying by the regulatory agency, and (c) protection of records. There are two common types of storage: file-based or relational database. Data in either format can be secured with the right system.

In addition to storage, laboratories must determine which data system topology is best for them (i.e., client/server or workstation). If a laboratory has more than three workstations, a centralized client/server topology is recommended for ease of data backup and advanced security. It is also the most economical solution.

> “Properly configuring technical controls enable data integrity and automate some business processes. OpenLab CDS allows laboratories to configure the right security policies for their users, specifically for password management.”

Key records of interest within analytical data systems to ensure data integrity are shown in **Figure 1**.

Technical controls. Properly configuring technical controls enable data integrity and automate some business processes. OpenLab CDS allows laboratories to configure the right security policies for their users, specifically for password management (**Figure 2**). Users can define and configure the minimum length of passwords, define password expiration periods, and define the minimum number of unsuccessful log-in attempts before an active user is blocked.

21 *CFR* Part 211.199(a)(8) states that original records must be reviewed by a second individual to ensure accuracy, completeness, and compliance. To satisfy this rule, OpenLab CDS has an enhanced e-signature feature to automate the data-review process within the electronic data system. During the creation and configuration of a project, users can customize the number of levels of review required for any batch approval. Users can also enforce e-signature order by locking the results from editing during the review and approval process. Same-level signatures for peer review can also be enabled.

Figure 1: Records of interest for any analytical data system.

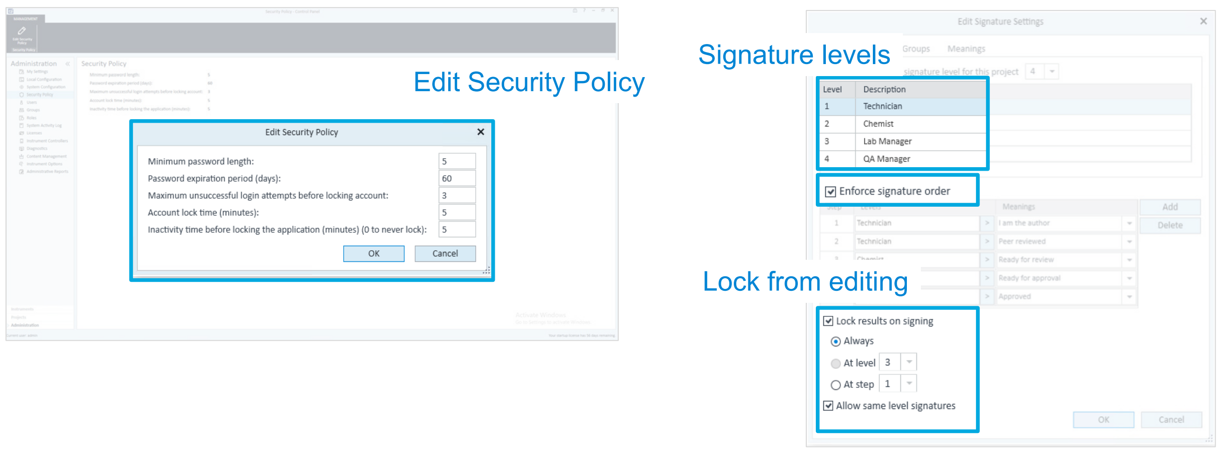
Key Records

- Instrument tune parameters
- Acquisition methods
- Acquired data
- Analysis/processing methods
- Analysis results – review + eSig
- Report templates
- Sequence template
- Executed sequence

Log/audit trails (Key Entries)

- Method audit trail
- Sequence audit trail
- Injection audit trail
- Result set audit trail
- Instrument activity log
- System activity log
- Injection log
- Result set log

Figure 2: Technical controls—security policy and signature settings.



Edit Security Policy

Edit Security Policy

Minimum password length:	5
Password expiration period (days):	60
Maximum unsuccessful login attempts before locking account:	3
Account lock time (minutes):	5
Inactivity time before locking the application (minutes) (0 to never lock):	5

Signature levels

Edit Signature Settings

Level	Description
1	Technician
2	Chemist
3	Lab Manager
4	QA Manager

☑ Enforce signature order

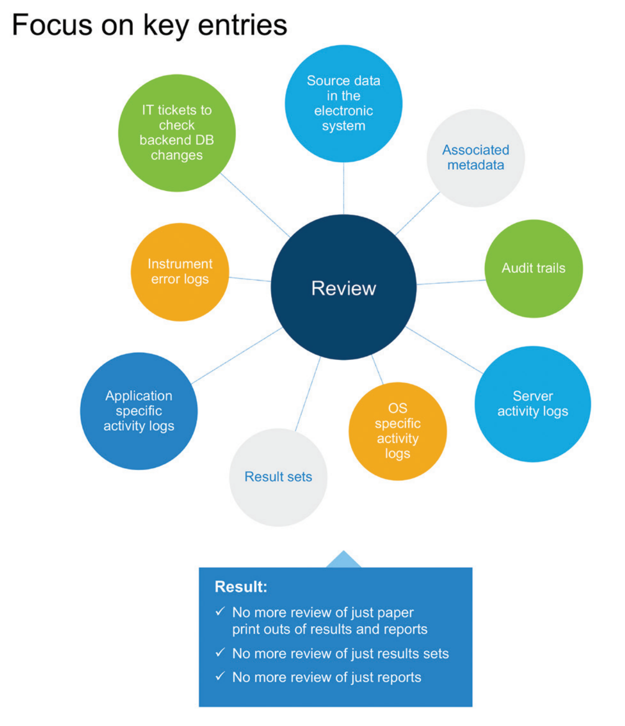
Lock from editing

☑ Lock results on signing
● Always
○ At level 3
○ At step 1
☑ Allow same level signatures

Paradigm Shift in Data Review

Historically, paper-based or paper-electronic hybrid laboratories released batches based on the review of results sets and printed reports. Regulators have since realized that with modern data systems, the review process that was historically in place was incomplete and inadequate. Now, regulators are focusing on data security and data integrity because of how easy it is to manipulate electronic records (see **Figure 3**).

Figure 3: Area of focus in the review process.



Focus on key entries
Source data in the electronic system
IT tickets to check backend DB changes
Associated metadata
Instrument error logs
Review
Audit trails
Application specific activity logs
OS specific activity logs
Server activity logs
Result sets

Result:

- ✓ No more review of just paper print outs of results and reports
- ✓ No more review of just results sets
- ✓ No more review of just reports

Along with the results sets and audit trails, regulators are looking at instrument error logs, application or system-specific activity logs, operating system-specific logs, and IT tickets for changes made by the database administrator to the back-end database (e.g., data manipulation or deletion).

It's not enough just to review reports and audit trails. Laboratories must look at all activity logs and audit trails as part of the review process. During audits they must show that they are actively reviewing data based on SOPs and demonstrate that they understand all entries in logs and audit trails.

Key Log Entries Generated by an Analytical Data System

Log file entries are generated and can be segregated based on instrument-related actions, system configurations, system security, system and user access, application-specific related activities along with actions and entries related to the recorded data set.

Instrument-related entries include:

- Calibration (tune events such as changes to tune parameters for mass spectrometers)
- Instrument maintenance events
- Changes to instrument settings made during runs
- Instrument configuration changes
- Errors (e.g., pressure, vacuum, lamp failures)
- Instrument warnings

Errors during the analytical run are a huge area of concern for auditors and regulatory inspectors. Auditors want to know what happened during the run and laboratories must be prepared to explain reasons for errors or changes made.

By reviewing these log file entries laboratories gain insight into their instrument control software, actions logged by the software, and potential instrument and results set issues.

System configuration entries include:

- Storage changes (type and location).
- System maintenance events
- Application auto-locking time
- Project creation and copying

No matter if a laboratory is moving current storage to the cloud, pointing systems to a different VM servers, or conducting system maintenance, the system log entries chronicle all the maintenance and application settings and subsequent changes usually per a laboratory's predefined internal specifications and plans.

Entries generated regarding system security include assigning the right privileges to each user and configuring the right policies for password management that follow best practices for maintaining the data integrity. It also includes changes made to project privileges, user access/privileges/passwords, and group privileges. By reviewing the log entries, changes made to user rules and privileges can be compared to laboratory SOPs.

When it comes to system and user access, auditors look at specific user activities with a particular system or instrument during a given timeframe. They look for users trying to perform actions that are not relevant or are not consistent with laboratory's SOPs. By reviewing these entries, stakeholders can track user activities within the system and verify if users are working as described in SOPs. Specifically, during the security audits, these entries are very relevant.

Understand Your Data System Workflow

A typical analytical data system workflow can be broken down into five phases:

Stage 1: Analytical prep method. Develop the right analytical methods to deliver the reliability, robustness, and accuracy of analytical measurements or choose an existing method that is qualified.

Stage 2: Single sample or sequence submission. The key records of interest are: sequence templates, acquisition methods, processing methods, sequence, instrument and system activity logs. Verify the right acquisition and processing methods have been used and verify the right vials and injection volume were selected. Defined SOPs must be followed.

> “Along with the results sets and audit trails, regulators are looking at instrument error logs, application or system-specific activity logs, operating system-specific logs, and IT tickets for changes made by the database administrator to the back-end database (e.g., data manipulation or deletion).”

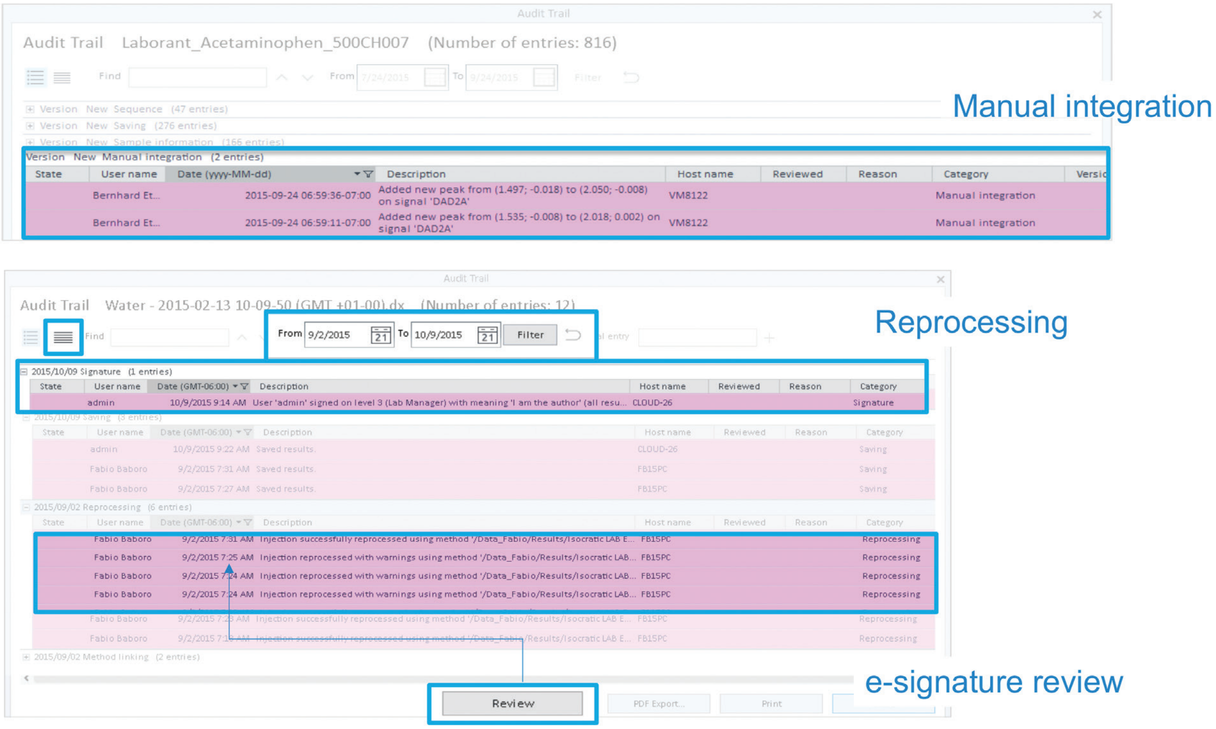
Stage 3: Data acquisition. In this phase, the application records the instrument signals and parameter settings. Instruments load the method parameters and the sample data are collected. The key records of interest are: raw data, chromatograms, spectra, sequence audit trail, instrument activity log, direct control actions, and system activity log.

Stage 4: Data analysis. In this stage, the system automatically applies processing method parameters that were selected during the sequence run submission to the acquired data. The key records of interest are: results set audit trail, processing method audit trail, injection audit trail, stored results, and custom calculations.

Stage 5: Reporting. In this stage, review any changes made to the report templates and make sure that the users making the changes have the right access privilege per the SOPs. The key records of interest are: report template audit trail, results set audit trail, processing method audit trail, injection audit trail, sequence summary report and custom calculations.

Figure 4 shows the OpenLab CDS audit trail. All the reprocessing entries are grouped together, and the reviewer can directly review entries in the audit trail using an e-signature as an acknowledgement. The review button is not enabled until the user scrolls down to complete review. It is color coded for clear differentiation between the reviewed and unreviewed entries. Manual integrations are also clearly labeled in the audit trail.

Figure 4: Audit trail.



Audit Trail Laborant_Acetaminophen_500CH007 (Number of entries: 816)

⊞ Version New Sequence (47 entries)
⊞ Version New Saving (276 entries)
⊞ Version New Sample information (166 entries)
Version New Manual integration (2 entries)

State	User name	Date (yyyy-MM-dd)	Description	Host name	Reviewed	Reason	Category	Versio
	Bernhard Et...	2015-09-24 06:59:36-07:00	Added new peak from (1.497; -0.018) to (2.050; -0.008) on signal 'DAD2A'	VM8122			Manual integration	
	Bernhard Et...	2015-09-24 06:59:11-07:00	Added new peak from (1.535; -0.008) to (2.018; 0.002) on signal 'DAD2A'	VM8122			Manual integration	

Audit Trail Water - 2015-02-13 10-09-50 (GMT +01-00).dx (Number of entries: 12)

⊟ 2015/10/09 Signature (1 entries)

State	User name	Date (GMT-06:00)	Description	Host name	Reviewed	Reason	Category
	admin	10/9/2015 9:14 AM	User 'admin' signed on level 3 (Lab Manager) with meaning 'I am the author' (all resu...	CLOUD-26			Signature

⊟ 2015/10/09 Saving (3 entries)

State	User name	Date (GMT-06:00)	Description	Host name	Reviewed	Reason	Category
	admin	10/9/2015 9:22 AM	Saved results.	CLOUD-26			Saving
	Fabio Baboro	9/2/2015 7:31 AM	Saved results.	FB15PC			Saving
	Fabio Baboro	9/2/2015 7:27 AM	Saved results.	FB15PC			Saving

⊟ 2015/09/02 Reprocessing (6 entries)

State	User name	Date (GMT-06:00)	Description	Host name	Reviewed	Reason	Category
	Fabio Baboro	9/2/2015 7:31 AM	Injection successfully reprocessed using method '/Data_Fabio/Results/Isocratic LAB E...	FB15PC			Reprocessing
	Fabio Baboro	9/2/2015 7:25 AM	Injection reprocessed with warnings using method '/Data_Fabio/Results/Isocratic LAB...	FB15PC			Reprocessing
	Fabio Baboro	9/2/2015 7:24 AM	Injection reprocessed with warnings using method '/Data_Fabio/Results/Isocratic LAB...	FB15PC			Reprocessing
	Fabio Baboro	9/2/2015 7:24 AM	Injection reprocessed with warnings using method '/Data_Fabio/Results/Isocratic LAB...	FB15PC			Reprocessing
	Fabio Baboro	9/2/2015 7:23 AM	Injection successfully reprocessed using method '/Data_Fabio/Results/Isocratic LAB E...	FB15PC			Reprocessing
	Fabio Baboro	9/2/2015 7:1[illegible] AM	Injection successfully reprocessed using method '/Data_Fabio/Results/Isocratic LAB E...	FB15PC			Reprocessing

⊞ 2015/09/02 Method linking (2 entries)

> “When it comes to system and user access, auditors look at specific user activities with a particular system or instrument during a given timeframe. They look for users trying to perform actions that are not relevant or are not consistent with laboratory’s SOPs.”

Some common data integrity and regulatory concerns are:

- Did stakeholders review changes made to the acquisition and processing methods (modified thresholds, purity, etc.) during the run?
- Are the right controls for preventing data falsification during data analysis or data processing set up?
- Did stakeholders investigate manual integrations?
- Have the appropriate users reviewed and approved the processed results sets with e-signatures, in the right order as defined in the laboratory SOPs?
- Were the custom calculations validated and reviewed?

Based on several recent 483s, regulators are most likely to be focused on Stages 3, 4, and 5.

Conclusion

Understand how your data systems work. Know when and what records are created in each step of the workflow; review the audit trails and activity log entries and be ready to explain any deviation that occurred during the different phases of the workflow. Don’t forget to utilize the tools offered by vendors such as the user documentation, online help, training service and white papers to be ready for your next internal or external audit.