Audit trails: Ensuring Data Integrity in the digital world

Reshma Kodumuru
Principal CSV Specialist
KBI Biopharma

About Presenter:

My name is **Reshma Kodumuru**. In my current role at KBI Biopharma, I lead a team of CSV Engineers to implement robust validation strategies that not only meet stringent regulatory requirements but also streamline processes for efficiency and effectiveness. My work is vital in closing gaps between compliance and innovation, enabling biopharma companies to bring safe, effective therapies to market faster.

Outside of work, I enjoy singing, which rejuvenates my spirit and keeps me grounded. I'm also a proud mother to a wonderful son, who inspires me every day to pursue excellence both professionally and personally.

+1(302)-407-2152
reshmakodumuru94@gmail.com

AGENDA

01 Introduction To Data Integrity and Audit Trails

02 Static Vs. Dynamic Data- The Evolution Of Data In Regulated Environment

03 ALCOA+ In The Context Of Dynamic Data- Understanding The Limitations

04 Introducing DYNAMIC + Framework: Moving Beyond ALCOA+ in Pharma 4.0

01

Introduction to Data Integrity and Audit Trails

What Is Data Integrity?

Definition:

Data Integrity refers to the accuracy, consistency, reliability, and security of data over its life cycle.

Why Is It Important?

ALCOA + Principles

Evolution From ALCOA To ALCOA+

Principle	ALCOA (Original)	ALCOA+ (Enhanced)
Attributable	Data should be traceable to the individual who recorded it	Includes accountability for modifications with audit trails
Legible	Data should be readable and permanent	Ensures long-term readability with metadata and contextual clarity.
Contemporaneous	Data should be recorded at the time of activity	Stresses real-time data entry with time stamps and automation
Original	Data should be in its original form or a certified copy.	Emphasizes integrity through digital records and validation.
Accurate	Data should be free of errors and reliable	Expands to include validation, cross-checks, and enhanced security.
Complete	-	Data must be whole, with no deletions or unexplained modifications.
Consistent	-	Data should follow a chronological order and a structured format.
Enduring	-	Data should be preserved and retrievable for its entire lifecycle.
Available	-	Data should be accessible when needed for regulatory review

What Are Audit Trails?

Definition: Audit trails are secure, time-stamped electronic records that document the sequence of activities or changes made to data within a system.

Audit Trails Typically Capture:

- WHO, WHAT, WHEN, WHY
- Before and after values of critical data points

Audit trails help in detecting unauthorized modifications, ensuring accountability, and maintaining data integrity, which are crucial for regulatory inspections and quality assurance.

Audit Trails Role In Data Integrity

Audit trails play a critical role in ensuring data integrity by maintaining an accurate, transparent and traceable record of all data related activities.

Data Integrity is fundamental for regulatory compliance, product quality, and patient safety. Here's how audit trails contribute to DI:

- Ensuring Data Traceability and Accountability
- Facilitating Investigations and Root Cause Analysis
- Enhancing Data Reliability and Accuracy
- Enabling Real-Time Monitoring and Quality Assurance

Overview Of Regulatory Bodies Governing Audit Trails

- FDA - Food and Drug Administration
- EMA -European Medicines Agency
- MHRA-Medicines and Healthcare products Regulatory Agency
- ICH-International Council for Harmonization

Overview Of Regulatory Bodies Governing Audit Trails

Regulatory Body	Computerized System Regulation	Audit Trail Requirement	Data Integrity Guidance Focus
FDA- Food and Drug Administration	21 CFR Part 11- Regulations on electronic records and electronic signatures	• Must record user actions, modifications, and deletions • Must be secure, time-stamped, and non-alterable • Readily retrievable for inspections	Focus on ALCOA+ Principles
EMA	Annex 11 (EU GMP)	• Requires audit trails for critical data modifications • Regular review of audit trails • Must be secure ad non-editable	Focuses on traceability, accountability, and compliance
MHRA	UK data Integrity Guidance	• Requires secure and accurate audit trails • Audit trails must be reviewed periodically	Identifies audit trails as critical GMP compliance
ICH	ICH-Q7 for APIs	• Electronic data must be protected from modifications • Audit trails must be reviewed regularly.	Data Security

Evolution Of Audit Trail Regulations In Pharmaceutical Industry

Pre-2000s

Paper based records keeping and minimal Electronic Regulation.

Early 2000s

Introduction of FDA 21 CFR Part 11

2010s

Global Regulatory Bodies Strengthen Audit Trail Guidelines

Late 2010s

Rising Data Integrity Issues Lead to Stricter Enforcement

2020s and Future

Automation AI, and Blockchain in Audit trails

Evolution of Audit Trail Regulations in Pharmaceutical Industry

Time Period	Regulatory Evolution	Impact
Pre-2000s	Paper based records, minimal electronic regulation	High risk of data loss and manipulation
Early 2000s	FDA 21 CFR Part 11 Introduction of Electronic Records and Electronic Signatures	Required Audit trails in computerized system
2010s	EMA Annex 11 introduced for EU GMP compliance and MHRA, WHO reinforced data integrity	Required audit trails in computerized systems. Stricter global enforcement and periodic audit trail reviews.
Late 2010s	Stricter enforcement due to data integrity breaches	More Focus on ALCOA+ Principles
2020s and future	AI Block chain, and real time monitoring	Automatic and predictive compliance for audit trails

02

Static Vs. Dynamic Data:
The Evolution Of Data In Regulated Environment

Static Vs. Dynamic Data- The Evolution Of Data In Regulated Environment

Static Data:

- Fixed unchanging data after recording
- Typically stored in databases, spreadsheets, or documents.
- Example: Signed paper records, PDFs, scanned lab records.

Dynamic Data:

- Continuously changing or modifiable data
- Often generated in real-time, requiring audit trails for compliance
- Example: Real-time sensor data, electronic batch records (EBRs).

Comparison: Static Vs Dynamic Data

Feature	**Static Data**	**Dynamic Data**
Nature	Fixed Unchangeable	Continuously evolving
Storage	Paper based, PDFs, structured databases	Cloud based, real-time logs, automated systems
Modification	Not editable post-entry	Frequently updated, requires version tracking
Compliance Needs	Traditional ALCOA Principles	Requires ALCOA+ with Dynamic data controls

Challenges with ALCOA+ for Dynamic Data

- ALCOA+ was originally designed for Static data integrity
- Challenges arise in ensuring:
    - Real time tracking and audit trails for frequent updates.
    - Security and access control for constantly changing data.
- Need for DYNAMIC + framework to bridge gaps.

03

ALCOA+ In The Context Of Dynamic Data- Understanding The Limitations

Limitations of ALCOA+ in a Dynamic Data Environment

- Designed for Linear Data- Lacks adaptability for non-sequential, evolving datasets
- Audit trail Changes- Difficulties in capturing frequent data changes
- Real time monitoring Struggles-Issues in tracking and maintaining multiple data versions
- Regulatory Gaps – Existing compliance models struggle to ensure DI in dynamic environments.

What is DYNAMIC+?
A Future Ready Framework

- Expands ALCOA+ to support real-time tracking, evolving, multi-source data
- Introduces versioning, automation, and AI driven compliance
- Enables cloud-native audit trails with automated tracking.

04

DYNAMIC+ Framework: Introducing DYNAMIC + Framework: Moving Beyond ALCOA+ in Pharma 4.0

What is DYNAMIC+ Framework?

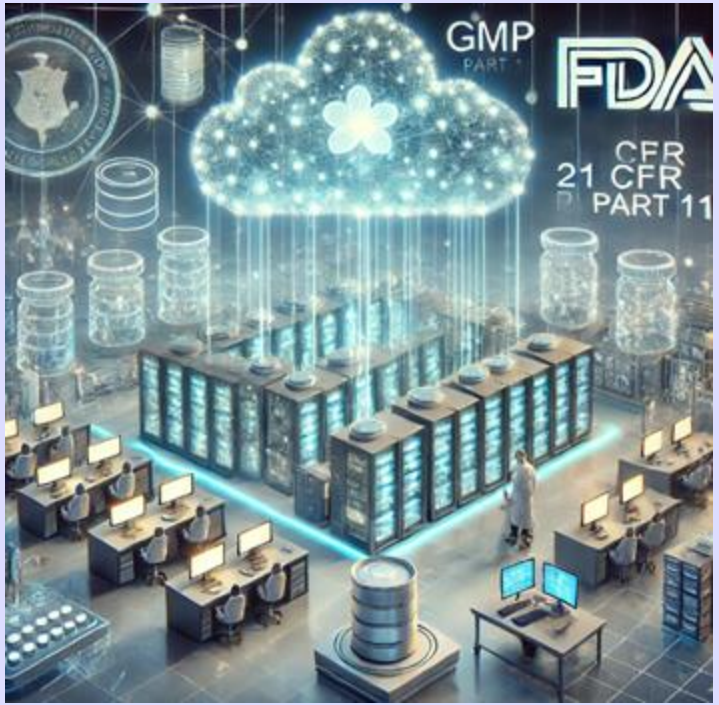
Principle	Definition	Why It's Needed in Pharma 4.0?
D - Decentralized	Ensures data integrity in distributed systems by leveraging cloud, blockchain, and edge computing.	Pharma 4.0 requires multi-site data accessibility and transparency, especially for global trials and supply chains.
Y - Yield-Driven	Aligns data integrity with business and compliance objectives, ensuring that all data contributes to process optimization.	Enables a performance-driven approach rather than a purely compliance-based one.
N - Non-Repudiable	Uses cryptographic security (blockchain, digital signatures) to prevent unauthorized alterations.	Prevents intentional data manipulation, fraud, and compliance violations.
A - Autonomous	Utilizes AI-driven compliance mechanisms to automate data validation, anomaly detection, and error correction.	Minimizes human intervention, ensuring real-time regulatory adherence.
M - Meta-Integrated	Captures metadata, audit logs, and AI-generated confidence scores to enhance traceability.	Improves visibility across AI-driven systems and digital workflows.
I - Interoperable	Ensures seamless data integrity across IoT devices, LIMS, MES, ERP, and other digital platforms.	Reduces data silos and enhances system-wide compliance.
C - Cognitive	Integrates AI-powered cognitive monitoring for continuous validation and predictive analytics.	Identifies compliance risks before they occur, reducing deviations and batch failures.
+ - Cybersecure & Continuous	Adopts zero-trust security models, end-to-end encryption, and real-time monitoring.	Ensures data availability while preventing cybersecurity threats.

D - Decentralized

Example: Cloud-Based Electronic Batch Records (EBR) in Global Manufacturing

- Ensures real-time traceability across multiple global locations.

- Reduces batch review time and improves efficiency.



Y - Yield-Driven

Example: AI-Driven Process Optimization in Vaccine Production

- AI optimizes manufacturing parameters in real-time.

- Reduces variability and maximizes production efficiency.

N - Non-Repudiable

Example: Blockchain for Tamper-Proof Clinical Trial Data

- Blockchain ensures immutable records of clinical trial data.

- Enhances compliance and builds stakeholder confidence.

A - Autonomous

Example: AI-Based Audit Trail Analysis in Laboratory Environments

- AI automates compliance monitoring and anomaly detection.

- Reduces audit review time by up to 80%.

M - Meta-Integrated

Example: End-to-End Bioprocessing Digital Twin Technology

• Real-time monitoring with integrated metadata.

• Enhances traceability and minimizes batch variations.

I - Interoperable

Example: Data Integrity Between LIMS, MES, and ERP Systems

- Ensures seamless data exchange across different platforms.

- Eliminates inconsistencies and improves regulatory compliance.

C - Cognitive

Example: AI-Driven Data Integrity Risk Forecasting

• AI predicts high-risk compliance issues before audits.

• Reduces regulatory notifications and enhances process efficiency.

+ - Cybersecure & Continuous

Example: Zero-Trust GxP Cloud Systems Cybersecurity

• Implements zero-trust security to prevent unauthorized access.

• Continuous monitoring ensures data confidentiality and compliance.

Any Questions?

Thank You!