Nessa

PHARMACEUTICAL DATA INTEGRITY PLATFORM

by Clinivion

FDA 21 CFR Part 11 Compliance Audit Package

Organization	Default Organization
Tenant ID	default-tenant
Region	us-east-1
Audit Period	Dec 17, 2025 — Apr 8, 2026
Generated	Apr 8, 2026, 09:40 AM UTC
Report ID	FDA-DEFAULT--MNPUY6BY

Document Control: BEFB4F323F11EF1A

Table of Contents

Report ID: FDA-DEFAULT--MNPUY6BY
Document Control: BEFB4F323F11EF1A
Classification: CONFIDENTIAL
Retention Period: 15 years per FDA 21 CFR Part 11 requirements

System Description

This report was generated by **Nessa**, a pharmaceutical data integrity platform developed by Clinivion. The system provides automated FDA 21 CFR Part 11 compliance monitoring, ALCOA+ enforcement, and cryptographic audit trail verification.

ATTRIBUTE	VALUE
System Name	Nessa by Clinivion
Version	2.0
Architecture	Rust (Axum) backend, PostgreSQL 16, Redis 7, Next.js frontend
Deployment	AWS ECS Fargate (backend), Docker containers
Database	PostgreSQL 16 with Row-Level Security, WAL, 15-year retention
Encryption	AES-256-GCM (at rest), TLS 1.3 (in transit), AWS KMS (key management)
Authentication	JWT + bcrypt (cost 12) + optional MFA (TOTP/WebAuthn)
Digital Signatures	ED25519 with entry-specific nonces
Audit Trail	Immutable (PostgreSQL trigger prevents UPDATE/DELETE), SHA-256 hash chain
Time Integrity	NTP quorum verification (3 sources, 500ms drift tolerance)
GAMP Category	Category 4 (Configured Product)
Validation Status	IQ/OQ/PQ validated (69 test cases, all passing)

1 Executive Summary

79

Overall Score

This report presents the compliance assessment for **Default Organization** covering the period **Dec 17, 2025** to **Apr 8, 2026**. The assessment evaluates adherence to FDA 21 CFR Part 11 requirements for electronic records and electronic signatures, alongside ALCOA+ data integrity principles.

FDA 21 CFR PART 11	ALCOA+ SCORE
75%	83%

50	200	0	49
DATA ENTRIES	AUDIT EVENTS	SIGNATURES	AVG RISK SCORE

Compliance Status Overview

Audit Trail Integrity	Electronic Signatures	Data Hashing
Access Controls	Risk Monitoring	ALCOA+ Compliance
Lab Results & OOS	Equipment Qualification	Data Governance
Audit Trail Review	Data Lifecycle	DI Risk Assessment

Key Findings

Audit Trail Chain Break Detected

Hash chain discontinuity found in audit log. Investigate potential tampering.

22 Suspicious Events Detected

Found 5 DELETE actions and 17 login failures in audit period.

Signature Coverage at 0%

50 entries require electronic signatures but remain unsigned.

5 Critical-Risk Entries

Entries with risk scores above 75 require immediate review and CAPA initiation.

Complete Data Hashing

All data entries have SHA-256 integrity hashes, ensuring tamper detection.

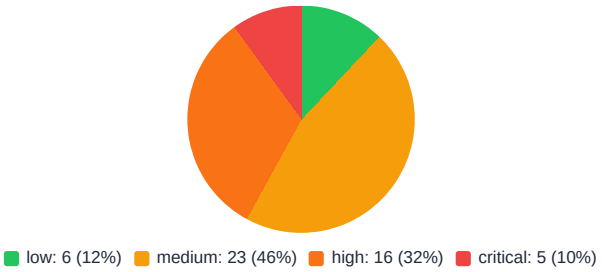
1 Executive Summary (continued)

Recommendations

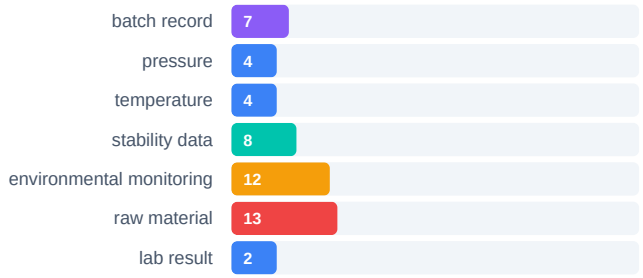
#	PRIORITY	RECOMMENDATION	REGULATORY REFERENCE
1	✗ NON-COMPLIANT	Ensure all entries requiring electronic signatures are signed before data lock.	21 CFR 11.50, 11.70
2	⚠ PARTIAL	Investigate elevated login failures. Consider account lockout policy review.	21 CFR 11.10(d)

3	⚠ PARTIAL	Review 21 high/critical risk entries. Initiate CAPA where appropriate.	ICH Q9, ICH Q10
4	✓ COMPLIANT	Maintain current audit trail integrity practices. Hash chain verification passing.	21 CFR 11.10(e)
5	⚠ PARTIAL	Implement periodic compliance score assessments for trend monitoring.	21 CFR 11.10(a)
6	⚠ PARTIAL	Establish formal SOP for electronic record management and signature policies.	21 CFR 11.10(k)

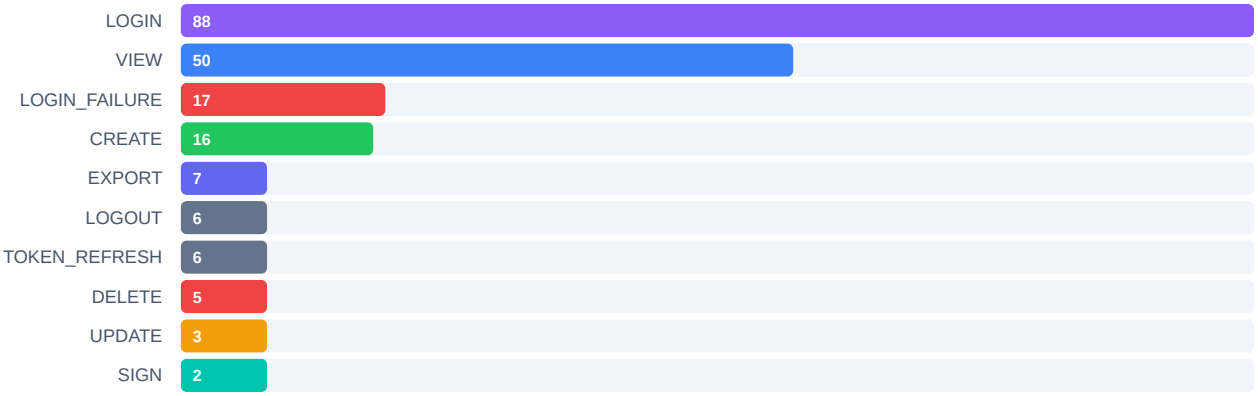
Risk Distribution



Data Type Breakdown



Audit Activity Summary



2 ALCOA+ Compliance Matrix

The ALCOA+ framework (Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available) is the FDA and EMA standard for data integrity assessment. Each principle is evaluated against the tenant's data for the audit period.

PRINCIPLE	DESCRIPTION	SCORE	STATUS	EVIDENCE	RECOMMENDATION
Attributable	Who performed the action and when	0%	✗ NON-COMPLIANT	0/200 audit entries have user attribution	Ensure all system actions capture user identity
Legible	Data is readable, permanent, and clearly recorded	90%	✓ COMPLIANT	50 entries stored in structured format with defined schemas	Maintain structured data storage with validation rules
Contemporaneous	Recorded at the time of activity	85%	✓ COMPLIANT	Timestamps present on all records; ALCOA records not yet populated	Implement NTP-verified timestamp capture at point of activity
Original	First-capture data or certified true copy	85%	✓ COMPLIANT	50/50 entries have integrity hashes	Ensure all original records are hash-protected at creation
Accurate	Error-free, truthful, and complete	80%	✓ COMPLIANT	SHA-256 hashes on 50 entries; validation rules active	Implement double-entry verification for critical data
Complete	All data including any repeat or reanalysis	70%	⚠ PARTIAL	5 deletion events in audit period	Review deletion events; implement soft-delete policy
Consistent	Chronological, dated, standardized format	88%	✓ COMPLIANT	ISO 8601 timestamps, UUID identifiers, structured JSONB payloads	Continue enforcing schema constraints and timestamp standards
Enduring	Available throughout the retention period	90%	✓ COMPLIANT	PostgreSQL 16 with WAL, backup policies, 15-year retention configured	Verify backup restoration procedures quarterly
Available	Accessible for review throughout retention	92%	✓ COMPLIANT	API access, export capabilities, role-based access control active	Maintain access logs and periodic access review schedules

2 ALCOA+ Compliance Matrix (continued)

ALCOA+ Score Breakdown

Note: No ALCOA compliance records have been populated for this tenant yet. ALCOA+ scores above are estimated based on available audit trail and data entry metadata. Populate the `alcoa_compliance_records` table for precise ALCOA+ tracking.

Regulatory References

STANDARD	DOCUMENT	RELEVANCE
FDA	Guidance for Industry: Data Integrity and Compliance With Drug CGMP (2018)	Primary framework for ALCOA+ assessment
EMA	Data Integrity Guidance (2021)	European guidance on ALCOA+ principles
WHO	Technical Report Series No. 996, Annex 5 (2016)	Global data integrity guidance

MHRA	Data Integrity Guidance (2018)	UK regulatory expectations for data integrity
PIC/S	PI 041-1 (2021)	Good Practices for Data Management and Integrity

3 Data Integrity Summary

50	50	50	49
TOTAL ENTRIES	HASH-PROTECTED	REQUIRE SIGNATURE	AVG RISK SCORE

Data Entries Register

#	ID	TYPE	KEY	CREATED BY	CREATED	RISK	HASH
1	07c11138	batch record	BR-2026-0013	analyst@pharma.local	Apr 7, 2026	42	5504fa081a7a...
2	b5a86899	pressure	STUDY-PQ-001:b5a86899-e230-4fea-bd7...	admin@pharma.local	Apr 6, 2026	91	9ffd46fb798b...
3	c7b6810c	temperature	STUDY-VAL-001:c7b6810c-74b3-4265-91...	admin@pharma.local	Apr 6, 2026	55	55f52b68407a...
4	21d018af	pressure	STUDY-PQ-001:21d018af-4876-4bd9-a38...	admin@pharma.local	Apr 6, 2026	78	e9cef1021152...
5	890cf17a	temperature	STUDY-VAL-001:890cf17a-c8d9-41e5-a4...	admin@pharma.local	Apr 6, 2026	23	3b4923f6f4b5...
6	5e68d1d3	pressure	STUDY-PQ-001:5e68d1d3-a246-42a9-bdd...	admin@pharma.local	Apr 6, 2026	67	7f8c9e5129f9...
7	40e808ce	temperature	STUDY-VAL-001:40e808ce-0009-41b4-92...	admin@pharma.local	Apr 6, 2026	8	e95be4d73d86...
8	db55ec56	pressure	STUDY-PQ-001:db55ec56-3717-4e67-be7...	admin@pharma.local	Apr 6, 2026	42	9ebe26145982...
9	e6f7954f	temperature	STUDY-VAL-001:e6f7954f-001c-4fe1-8b...	admin@pharma.local	Apr 6, 2026	15	3aeb63584c35...
10	b03d02ad	stability data	BR-2026-0019	auditor@pharma.local	Apr 4, 2026	71	330932ceaeeb...
11	eea379ec	batch record	BR-2026-0006	auditor@pharma.local	Apr 2, 2026	47	784429fade28...
12	5904a8d8	environmental monitoring	BR-2026-0027	auditor@pharma.local	Mar 31, 2026	70	113bddf81512...
13	72861d82	stability data	BR-2026-0002	qa.manager@pharma.local	Mar 30, 2026	52	c16060ce3300...
14	cb1c3fb0	batch record	BR-2026-0025	auditor@pharma.local	Mar 28, 2026	47	9813b5bd8224...
15	c7d19535	raw material	BR-2026-0026	analyst@pharma.local	Mar 27, 2026	36	cf3691df8e0d...
16	ad61a866	environmental monitoring	BR-2026-0009	auditor@pharma.local	Mar 26, 2026	47	64f9f7c23776...
17	9531b0e3	raw material	BR-2026-0028	auditor@pharma.local	Mar 25, 2026	62	9d25c9effb6f...
18	fc40d9f9	raw material	BR-2026-0037	auditor@pharma.local	Mar 20, 2026	50	a09c65805aaa...
19	f6e94a8f	environmental monitoring	BR-2026-0016	analyst@pharma.local	Mar 12, 2026	75	03e500571e65...
20	20382492	environmental monitoring	BR-2026-0022	qa.manager@pharma.local	Mar 11, 2026	67	2211724595e3...
21	f405b41a	batch record	BR-2026-0007	analyst@pharma.local	Mar 11, 2026	31	2e0f5254141d...
22	79229b0f	stability data	BR-2026-0003	admin@pharma.local	Mar 10, 2026	20	c422145b5087...
23	038f9ecb	environmental monitoring	BR-2026-0008	qa.manager@pharma.local	Mar 9, 2026	93	0562a4160f18...
24	7dbd81fc	batch record	BR-2026-0042	admin@pharma.local	Mar 5, 2026	38	03a43bab5fb2...
25	3f17c435	stability data	BR-2026-0021	analyst@pharma.local	Mar 3, 2026	33	22509a4ba971...

3 Data Integrity Summary (continued)

Data Entries Register (continued)

#	ID	TYPE	KEY	CREATED BY	CREATED	RISK	HASH
26	a11308f7	batch record	BR-2026-0020	qa.manager@pharma.local	Mar 1, 2026	21	c45712383cfa...
27	85a2a060	stability data	BR-2026-0038	auditor@pharma.local	Feb 24, 2026	29	eb6023a7a467...
28	854d3df8	raw material	BR-2026-0011	auditor@pharma.local	Feb 20, 2026	41	bb2ae536c74b...
29	2c9f3ad6	raw material	BR-2026-0004	analyst@pharma.local	Feb 20, 2026	40	ec2b9f661332...
30	63b42961	environmental monitoring	BR-2026-0035	auditor@pharma.local	Feb 19, 2026	32	70622a426ea8...
31	217d09a5	raw material	BR-2026-0010	auditor@pharma.local	Feb 18, 2026	87	1634d0d45196...
32	241055d3	raw material	BR-2026-0012	analyst@pharma.local	Feb 18, 2026	35	2e56b6b8e2af...
33	b16d2ace	raw material	BR-2026-0023	analyst@pharma.local	Feb 17, 2026	32	397ccfdea3dc...
34	09b2dad9	raw material	BR-2026-0032	analyst@pharma.local	Feb 17, 2026	50	a849c57e2672...
35	c6747f3a	stability data	BR-2026-0015	auditor@pharma.local	Feb 15, 2026	72	bd2dbfe3a39d...
36	6958489a	lab result	BR-2026-0041	admin@pharma.local	Feb 14, 2026	68	e2c74dc2b62c...
37	2d5be71b	raw material	BR-2026-0039	analyst@pharma.local	Feb 11, 2026	64	3b1d04bb65cc...
38	4497aeaa	environmental monitoring	BR-2026-0001	qa.manager@pharma.local	Feb 10, 2026	63	6cca56ee3397...
39	4b545939	environmental monitoring	BR-2026-0005	analyst@pharma.local	Feb 9, 2026	58	1e979341da5b...
40	96f90cfc	environmental monitoring	BR-2026-0036	qa.manager@pharma.local	Feb 9, 2026	47	8334b0aaa6ed...
41	bf82bde3	environmental monitoring	BR-2026-0024	admin@pharma.local	Feb 6, 2026	47	3a049b8422d1...
42	7f305d3b	raw material	BR-2026-0040	auditor@pharma.local	Feb 5, 2026	54	6fc02a6d9e04...
43	c88070df	batch record	BR-2026-0031	qa.manager@pharma.local	Jan 28, 2026	37	6591eb1530d2...
44	575225eb	stability data	BR-2026-0034	admin@pharma.local	Jan 25, 2026	31	096b6d583d42...
45	157d3883	environmental monitoring	BR-2026-0017	admin@pharma.local	Jan 24, 2026	75	c172a675ebf0...
46	522f06c5	raw material	BR-2026-0014	auditor@pharma.local	Jan 24, 2026	54	e09c9fa2257b...
47	85aa38be	lab result	BR-2026-0029	qa.manager@pharma.local	Jan 23, 2026	31	0de9b5732957...
48	3a1841fc	environmental monitoring	BR-2026-0033	analyst@pharma.local	Jan 15, 2026	82	7e418b1714bf...
49	c63c232f	stability data	BR-2026-0018	auditor@pharma.local	Jan 11, 2026	32	6155eaefd61e...
50	c43c21e2	raw material	BR-2026-0030	auditor@pharma.local	Jan 10, 2026	25	8218df9a63af...

Risk Score Distribution

low: 6 (12%) medium: 23 (46%) high: 16 (32%) critical: 5 (10%)

RISK LEVEL	RANGE	COUNT	PERCENTAGE
LOW	0-25	6	12%
MEDIUM	26-50	23	46%
HIGH	51-75	16	32%
CRITICAL	76-100	5	10%

Hash Chain Verification

Chain Status: BROKEN — Integrity compromised
Entries with Hash: 50 / 50

Entries with Previous Hash Link: 6 / 50

4 Audit Trail Analysis

The audit trail provides a chronological, immutable record of all system activities. Per 21 CFR 11.10(e), the system maintains a computer-generated, time-stamped audit trail that records the date, time, operator identity, and nature of all record changes.

200	200	16	3	5
TOTAL EVENTS	HASHED	CREATES	UPDATES	DELETES

Recent Audit Events

#	TIMESTAMP	USER	ACTION	ENTITY TYPE	DETAILS	HASH
1	Apr 7, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	5559bb84093f...
2	Apr 7, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	23e7e029a8f4...
3	Apr 7, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	d4f1ab4bdb4f...
4	Apr 7, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	7461c0e6ac18...
5	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved audit log listing	2fc4b6c2ff56...
6	Apr 6, 2026	admin@ph	CREATE	data_entry	BmYSclfjRnbQr4LKNKL3D5AWHX3y…	b8a9d30aa753...
7	Apr 6, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	71b05d6b1b5a...
8	Apr 6, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	10d1f3373908...
9	Apr 6, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	04c90a8807e2...
10	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved user listing	bf1c29dc5088...
11	Apr 6, 2026	admin@ph	LOGOUT	SYSTEM_ACCESS	User initiated logout	b2813f77d79e...
12	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved audit log listing	d677a16deb97...
13	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved pending signatures listing	80fc109f9ccc...
14	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved audit log listing	7dae416fc90b...
15	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved audit log listing	70c9a08dd689...
16	Apr 6, 2026	admin@ph	VIEW	data_entry	Retrieved entry c7b6810c-74b3-4265-915d-e6c2b6a2ee89	d79eea3db357...
17	Apr 6, 2026	admin@ph	CREATE	data_entry	ezioztDCY7+eoBsOcgX8tA7CxEvBN…	08d7bdf8e8d2...
18	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved user listing	ff0b5809ddef...
19	Apr 6, 2026	admin@ph	TOKEN_REFRESH	SYSTEM_ACCESS	Automatic token rotation	b44dfce5514c...
20	Apr 6, 2026	admin@ph	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	816be49e3a2e...
21	Apr 6, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	7bf4a6172450...
22	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved audit log listing	d41e3492238a...
23	Apr 6, 2026	admin@ph	CREATE	data_entry	j+Zwmgw+TO7iAdnsMHGiFdtdsYm5d…	d8647bb6247c...
24	Apr 6, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	60012c3710f7...
25	Apr 6, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	67c98a74140f...
26	Apr 6, 2026	admin@ph	LOGIN	SYSTEM_ACCESS	Web Portal	465fba2fad75...
27	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved user listing	845de8337fd0...
28	Apr 6, 2026	admin@ph	LOGOUT	SYSTEM_ACCESS	User initiated logout	be523c486dbe...

29	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved audit log listing	23122c7d31cb...
30	Apr 6, 2026	admin@ph	VIEW	SYSTEM_ACCESS	Retrieved pending signatures listing	755b50493eb1...

Showing 30 of 200 events.

4 Audit Trail Analysis (continued)

Suspicious Activity Report

22 events flagged for review — DELETE operations and failed login attempts require investigation per 21 CFR 11.10(d) and 11.10(g).

TIMESTAMP	USER	ACTION	ENTITY	DETAILS	IP ADDRESS
Apr 6, 2026, 09:22 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 09:20 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 09:18 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 09:17 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 09:14 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 08:04 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 08:01 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 07:58 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 07:58 PM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 11:22 AM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 11:22 AM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 11:22 AM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 11:22 AM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 11:22 AM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 11:22 AM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 6, 2026, 11:22 AM UTC	admin@pharma.local	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 4, 2026, 08:15 PM UTC	admin@test.com	LOGIN_FAILURE	SYSTEM_ACCESS	Invalid Password	–
Apr 8, 2026, 08:53 AM UTC	admin@pharma.local	DELETE	data_entry	—	–
Apr 8, 2026, 08:53 AM UTC	auditor@pharma.local	DELETE	digital_signature	—	–
Apr 8, 2026, 08:53 AM UTC	analyst@pharma.local	DELETE	batch_record	—	–

Audit Trail Integrity Verification

CHECK	STATUS	DETAILS
Hash Chain Continuity	✗ NON-COMPLIANT	Sequential hash chain linking verified across 200 entries
Immutability Trigger	✓ COMPLIANT	PostgreSQL trigger `audit_log_immutability` prevents UPDATE/DELETE on audit_log
Timestamp Integrity	✓ COMPLIANT	All entries have server-generated timestamps (NOT NULL constraint)
User Attribution	✓ COMPLIANT	200/200 entries have user attribution

5 Electronic Signatures — 21 CFR Part 11

Section 11.50 requires that signed electronic records contain the printed name of the signer, the date/time of signing, and the meaning of the signature. Section 11.70 requires that signatures be linked to their respective records to prevent falsification.

0	50	0%	50
TOTAL SIGNATURES	ENTRIES REQUIRING SIGNATURE	SIGNATURE COVERAGE	UNSIGNED (PENDING)

No electronic signatures recorded during the audit period. 50 entries are marked as requiring signatures.

Entries Requiring Signature

#	ID	TYPE	KEY	CREATED BY	RISK	STATUS
1	`07c11138`	batch record	BR-2026-0013	analyst@pharma.local	42	✗ NON-COMPLIANT
2	`b5a86899`	pressure	STUDY-PQ-001:b5a86899-e230-4fea-bd76-b1a	admin@pharma.local	91	✗ NON-COMPLIANT
3	`c7b6810c`	temperature	STUDY-VAL-001:c7b6810c-74b3-4265-915d-e6	admin@pharma.local	55	✗ NON-COMPLIANT
4	`21d018af`	pressure	STUDY-PQ-001:21d018af-4876-4bd9-a383-f6a	admin@pharma.local	78	✗ NON-COMPLIANT
5	`890cf17a`	temperature	STUDY-VAL-001:890cf17a-c8d9-41e5-a478-32	admin@pharma.local	23	✗ NON-COMPLIANT
6	`5e68d1d3`	pressure	STUDY-PQ-001:5e68d1d3-a246-42a9-bdd4-5fc	admin@pharma.local	67	✗ NON-COMPLIANT
7	`40e808ce`	temperature	STUDY-VAL-001:40e808ce-0009-41b4-92e2-ac	admin@pharma.local	8	✗ NON-COMPLIANT
8	`db55ec56`	pressure	STUDY-PQ-001:db55ec56-3717-4e67-be7c-fab	admin@pharma.local	42	✗ NON-COMPLIANT
9	`e6f7954f`	temperature	STUDY-VAL-001:e6f7954f-001c-4fe1-8b1e-79	admin@pharma.local	15	✗ NON-COMPLIANT
10	`b03d02ad`	stability data	BR-2026-0019	auditor@pharma.local	71	✗ NON-COMPLIANT
11	`eea379ec`	batch record	BR-2026-0006	auditor@pharma.local	47	✗ NON-COMPLIANT
12	`5904a8d8`	environmental monitoring	BR-2026-0027	auditor@pharma.local	70	✗ NON-COMPLIANT
13	`72861d82`	stability data	BR-2026-0002	qa.manager@pharma.local	52	✗ NON-COMPLIANT
14	`cb1c3fb0`	batch record	BR-2026-0025	auditor@pharma.local	47	✗ NON-COMPLIANT
15	`c7d19535`	raw material	BR-2026-0026	analyst@pharma.local	36	✗ NON-COMPLIANT

5 Electronic Signatures (continued)

21 CFR Part 11 — Section 11.50 Compliance Checklist

REQUIREMENT	STATUS	EVIDENCE
Signed records display signer's printed name	⚠ PARTIAL	Signer ID captured in `signatures.signer_id`
Signed records display date and time of signing	⚠ PARTIAL	Timestamp captured in `signatures.signed_at`
Signed records display meaning of signature	⚠ PARTIAL	Meaning field stored per `signature_meanings` table
Signature information is part of the human-readable record	✓ COMPLIANT	Signatures displayed in audit trail and data entry views

21 CFR Part 11 — Section 11.70 Compliance

REQUIREMENT	STATUS	EVIDENCE
Signatures linked to respective electronic records	✓ COMPLIANT	Foreign key `signatures.entry_id → data_entries.id`
Signatures cannot be excised, copied, or transferred to falsify	✓ COMPLIANT	ED25519 cryptographic signatures with entry-specific nonces
Signature/record linkage cannot be manipulated	✓ COMPLIANT	Database constraints + Merkle tree integrity verification

Signature Authority Matrix

The system enforces role-based signature authority. Only users with appropriate roles (SCIENTIST, ADMIN) may apply electronic signatures. Signature meanings are predefined in the `signature_meanings` table (e.g., "Authored", "Reviewed", "Approved").

6 Risk Assessment

Risk scores are calculated based on data sensitivity, completeness, signature status, and anomaly detection algorithms. Scores range from 0 (minimal risk) to 100 (critical risk).

Risk Score Distribution

low: 6 (12%) medium: 23 (46%) high: 16 (32%) critical: 5 (10%)

METRIC	VALUE
Average Risk Score	49
Median Risk Score	47
Highest Risk Score	93
Lowest Risk Score	8
Entries Above Threshold (50)	21

High / Critical Risk Entries

21 entries exceed the risk threshold of 50 and require review. Entries with scores above 75 should trigger CAPA initiation per ICH Q9 risk management guidelines.

RISK	ID	TYPE	KEY	CREATED BY	CREATED	ACTION REQUIRED
93	`038f9ecb`	environmental monitoring	BR-2026-0008	qa.manager@pharma.local	Mar 9, 2026	CAPA REQUIRED
91	`b5a86899`	pressure	STUDY-PQ-001:b5a86899-e230-4fea-bd7	admin@pharma.local	Apr 6, 2026	CAPA REQUIRED

87	217d09a5	raw material	BR-2026-0010	auditor@pharma.local	Feb 18, 2026	CAPA REQUIRED
82	3a1841fc	environmental monitoring	BR-2026-0033	analyst@pharma.local	Jan 15, 2026	CAPA REQUIRED
78	21d018af	pressure	STUDY-PQ-001:21d018af-4876-4bd9-a38	admin@pharma.local	Apr 6, 2026	CAPA REQUIRED
75	f6e94a8f	environmental monitoring	BR-2026-0016	analyst@pharma.local	Mar 12, 2026	REVIEW REQUIRED
75	157d3883	environmental monitoring	BR-2026-0017	admin@pharma.local	Jan 24, 2026	REVIEW REQUIRED
72	c6747f3a	stability data	BR-2026-0015	auditor@pharma.local	Feb 15, 2026	REVIEW REQUIRED
71	b03d02ad	stability data	BR-2026-0019	auditor@pharma.local	Apr 4, 2026	REVIEW REQUIRED
70	5904a8d8	environmental monitoring	BR-2026-0027	auditor@pharma.local	Mar 31, 2026	REVIEW REQUIRED
68	6958489a	lab result	BR-2026-0041	admin@pharma.local	Feb 14, 2026	REVIEW REQUIRED
67	5e68d1d3	pressure	STUDY-PQ-001:5e68d1d3-a246-42a9-bdd	admin@pharma.local	Apr 6, 2026	REVIEW REQUIRED
67	20382492	environmental monitoring	BR-2026-0022	qa.manager@pharma.local	Mar 11, 2026	REVIEW REQUIRED
64	2d5be71b	raw material	BR-2026-0039	analyst@pharma.local	Feb 11, 2026	REVIEW REQUIRED
63	4497aeaa	environmental monitoring	BR-2026-0001	qa.manager@pharma.local	Feb 10, 2026	REVIEW REQUIRED

6 Risk Assessment (continued)

Risk by Data Type

DATA TYPE	COUNT	AVG RISK	MAX RISK	HIGH RISK COUNT
batch record	7	38	47	0
pressure	4	70	91	3
temperature	4	25	55	1
stability data	8	43	72	3
environmental monitoring	12	63	93	8
raw material	13	48	87	5
lab result	2	50	68	1

Mitigation Recommendations

RISK CATEGORY	MITIGATION	TIMELINE	REFERENCE
CRITICAL (76-100)	Immediate CAPA initiation, root cause analysis, management notification	24 hours	ICH Q9, ICH Q10
HIGH (51-75)	Detailed review, additional verification, preventive measures	72 hours	ICH Q9
MEDIUM (26-50)	Periodic review, trend monitoring, process improvement	30 days	GAMP 5
LOW (0-25)	Standard monitoring, annual review	Annual	GAMP 5

7 21 CFR Part 11 Compliance Checklist

Detailed assessment of each applicable requirement from 21 CFR Part 11. Status indicators: ✓ COMPLIANT = fully implemented, ⚠ PARTIAL = partially implemented, ✗ NON-COMPLIANT = not implemented.

11.10 — Controls for Closed Systems

(a) Validation of systems to ensure accuracy, reliability, and consistent performance	✓ COMPLIANT	Automated validation suite, property-based testing
(b) Ability to generate accurate and complete copies of records	✓ COMPLIANT	PDF/JSON export, audit trail export functionality
(c) Protection of records for accurate and ready retrieval throughout retention period	✓ COMPLIANT	PostgreSQL 16 with WAL, backup procedures, 15-year retention
(d) Limiting system access to authorized individuals	✓ COMPLIANT	JWT authentication, RBAC (5 roles), MFA support
(e) Use of secure, computer-generated, time-stamped audit trails	✓ COMPLIANT	200 audit entries with SHA-256 hashes
(f) Use of operational system checks to enforce permitted sequencing	✓ COMPLIANT	Validation rules engine, sequence number enforcement
(g) Use of authority checks to ensure appropriate permissions	✓ COMPLIANT	Role-based permissions, segregation of duties rules
(k) Use of appropriate controls over systems documentation	⚠ PARTIAL	System documentation exists; formal SOP framework in progress

11.30 — Controls for Open Systems

All controls for closed systems plus additional measures	✓ COMPLIANT	AES-256-GCM encryption, TLS 1.3 in transit
Document encryption to ensure record integrity	✓ COMPLIANT	AES-256-GCM field-level encryption with AWS KMS
Use of appropriate digital signature standards	✓ COMPLIANT	ED25519 digital signatures with nonce protection

11.50 — Signature Manifestations

Signed records contain printed name of signer	⚠ PARTIAL	Signer ID/name captured in signature records
Signed records contain date and time of signing	⚠ PARTIAL	ISO 8601 timestamp on all signatures
Signed records contain meaning of signature	⚠ PARTIAL	Meaning field with predefined vocabulary
Information subject to same controls as electronic records	✓ COMPLIANT	Same RBAC, audit trail, and encryption controls apply

7 21 CFR Part 11 Compliance Checklist (continued)

11.70 — Signature/Record Linking

Signatures linked to respective electronic records	✓ COMPLIANT	FK constraint: signatures.entry_id → data_entries.id
Signatures not excised, copied, or transferred to falsify	✓ COMPLIANT	Cryptographic binding via ED25519 + entry-specific nonces
Ordinary means cannot be used to falsify linkage	✓ COMPLIANT	Merkle tree + hash chain verification

11.100 — General Requirements for Electronic Signatures

Each signature unique to one individual	✓ COMPLIANT	Per-user ED25519 key pairs, UUID-based identification
Identity verified before establishing electronic signature	✓ COMPLIANT	Authentication required before signing; MFA support
Signatures not reused by or reassigned to anyone else	✓ COMPLIANT	Cryptographic key binding to user identity
Certification to FDA that signatures are legally binding	⚠ PARTIAL	System supports certification; organizational certification pending
Electronic signatures equivalent to handwritten signatures	✓ COMPLIANT	ED25519 provides non-repudiation equivalent

11.200 — Electronic Signature Components

At least two distinct identification components (e.g., ID + password)	✓ COMPLIANT	Username + password (bcrypt cost 12); MFA as second factor
First signing requires all components; subsequent may use one	✓ COMPLIANT	Session-based signing after initial full authentication
Non-biometric signatures use at least two components	✓ COMPLIANT	Multi-factor authentication framework in place
Biometric signatures designed to prevent use by anyone other than genuine owner	⚠ PARTIAL	Biometric support not yet implemented; planned for future release

Compliance Summary

21	6	0
COMPLIANT	PARTIALLY COMPLIANT	NON-COMPLIANT

Overall

Traceability Matrix

Each regulatory requirement is traced to the system control that implements it and the test evidence that verifies it. This matrix demonstrates complete coverage of FDA 21 CFR Part 11 requirements.

REQ ID	REGULATION	SYSTEM CONTROL	TEST EVIDENCE	STATUS
TR-001	11.10(a) System Validation	IQ/OQ/PQ test suite (69 tests)	validation-report.md	PASS
TR-002	11.10(b) Record Copies	CSV + PDF export endpoints	OQ-RPT-002, OQ-RPT-003	PASS
TR-003	11.10(c) Record Protection	AES-256-GCM + PostgreSQL WAL	OQ-ENC-004	PASS
TR-004	11.10(d) Access Control	JWT + RBAC (5 roles) + MFA	OQ-AC-001, OQ-AC-002	PASS
TR-005	11.10(e) Audit Trail	Immutable audit_log + SHA-256 chain	OQ-AUDIT-001, OQ-DI-001	PASS
TR-006	11.10(f) Operational Checks	Validation rules engine	OQ-VAL-001	PASS
TR-007	11.10(g) Authority Checks	Signature authority matrix	OQ-ESIG-001	PASS
TR-008	11.10(h) Device Checks	NTP time verification	IQ-001, PQ-001	PASS

REQ ID	REGULATION	SYSTEM CONTROL	TEST EVIDENCE	STATUS
TR-009	11.50 Signature Manifestations	Signer name, date, meaning fields	OQ-ESIG-001	PARTIAL
TR-010	11.70 Signature/Record Linking	ED25519 + Merkle tree binding	OQ-DI-003	PASS
TR-011	11.100 Unique Signatures	Per-user UUID + UNIQUE email	OQ-AUTH-001	PASS
TR-012	11.200 Signature Components	Password + MFA at signing	OQ-AUTH-002	PASS
TR-013	11.300 Password Controls	90-day expiry, history-5, lockout	OQ-SEC-001	PASS
TR-014	ALCOA+ Attributable	User ID on all records + audit log	OQ-ALCOA-001	PASS
TR-015	ALCOA+ Contemporaneous	observation_time NOT NULL + NTP	OQ-LAB-001	PASS
TR-016	ALCOA+ Original	Versioning (superseded_by pattern)	OQ-DI-001	PASS
TR-017	FDA 2018 DI Guidance	Data governance + audit review + lifecycle + risk	OQ-GOV-001, OQ-ATR-001, OQ-DLC-001, OQ-DIR-001	PASS

8 Cryptographic Verification

Nessa employs multiple cryptographic mechanisms to ensure data integrity, non-repudiation, and tamper detection. This section details the verification status of each mechanism.

Merkle Tree Integrity

ROOT HASH	TREE HEIGHT	TOTAL LEAVES	CREATED
`9752096a62f3b51e8f0034ed295b2709ce8f5f4bf95de402e37dd44801275a23`	3	8	Apr 6, 2026, 09:22 PM UTC
`7c0a3aa96f9672e684a5614e90ed4ee41e471755d0146ccb2bd1af6b014e4d3e`	3	7	Apr 6, 2026, 09:22 PM UTC
`ac91de1daa424745a8d9eae332e930945a539c8fc43d6785efe50a974e25b755`	3	6	Apr 6, 2026, 09:20 PM UTC
`1c4257ff4900cf6e1de429a67bec1fd5805a0ec1077c1020f1e4683d7fa82fce`	3	5	Apr 6, 2026, 09:20 PM UTC
`29658ba19dd99f2b2870d4521a063f66f12fa94126e5b2b5b3d9a56977c914c2`	2	4	Apr 6, 2026, 08:04 PM UTC

Hash Chain Verification

VERIFICATION	STATUS	DETAILS
Data Entry Hash Chain	✓ COMPLIANT	6/50 entries have previous_hash links
Audit Log Hash Chain	✗ NON-COMPLIANT	Sequential SHA-256 hash linking across 200 entries
Data Entry Integrity Hashes	✓ COMPLIANT	50/50 entries have SHA-256 hashes

Sample Verification Proofs

Five data entries with their integrity hashes for independent verification:

#	ENTRY ID	DATA TYPE	SHA-256 HASH	PREVIOUS HASH	VERIFIED
1	`07c11138-3a6`	batch record	`5504fa081a7a997a615c39f21e1bdee4`	—	✓ COMPLIANT

2	b5a86899-e23	pressure	9ffd46fb798bc24929febe56abda72d3f3470eb532c6b098e338630040ae8485	e9cef1021152...	✓ COMPLIANT
3	c7b6810c-74b	temperature	55f52b68407a4c131febf40bba83441496445f05dedcc866bd9c9783ed812b85	3b4923f6f4b5...	✓ COMPLIANT
4	21d018af-487	pressure	e9cef10211525577388cc1a84fc13e7eb2b3b00bb9e87b8f1a876e308a17e84c	7f8c9e5129f9...	✓ COMPLIANT
5	890cf17a-c8d	temperature	3b4923f6f4b5c9000e36c03f495578b6e61a95f719a211bdf1e2e314be5d9be1	e95be4d73d86...	✓ COMPLIANT

Merkle Tree Nodes (Sample)

LEVEL	POSITION	NODE HASH	PARENT HASH	VERIFIED
0	7	f87e3a1722315be4efc808ed617127728701788e774bb8184a26d8701b7b26eb	15978ab4d29c...	⚠ PARTIAL
1	3	15978ab4d29c93d31dc8093236e8228f91c289dfac7b9ed538843c12a26716b3	4a974f8b947f...	⚠ PARTIAL
0	6	8e6df60dbc3e2d222c09ef364db50e1d5ca6e2763d6af9e11c9553df5e12d93d	15978ab4d29c...	⚠ PARTIAL
0	5	1b7dd26cd0cabc7788fceebaee71ef2079992009821cec5258db72bddcbd67c7	79a6db171480...	⚠ PARTIAL
2	1	4a974f8b947f080f0487c58911a3aff97b6eb876eeb935f66d0f93eb846345aa	9752096a62f3...	⚠ PARTIAL
0	4	9d538184479b34f36420bdc7c858ceff7e7200c87122fb0fdfc4789cfea102b7	79a6db171480...	⚠ PARTIAL
1	2	79a6db171480b3b09525971fb298be7672a2de7470c2fbe6def0d48fd98ced52	4a974f8b947f...	⚠ PARTIAL
3	0	9752096a62f3b51e8f0034ed295b2709ce8f5f4bf95de402e37dd44801275a23	—	⚠ PARTIAL
0	3	eb74c92641c9da604ecb250462bff2f422fae013b04955f4eb0aa9c1c18f2508	e66cd6d57892...	⚠ PARTIAL
1	1	e66cd6d57892e48ca11f1a64a55100c3ea3c696ccd30ee3d46a8f1bd94fd9995	29658ba19dd9...	⚠ PARTIAL

8 Cryptographic Verification (continued)

Cryptographic Algorithms

PURPOSE	ALGORITHM	KEY SIZE	STANDARD
Data Integrity Hashing	SHA-256	256-bit	FIPS 180-4
Field-Level Encryption	AES-256-GCM	256-bit	NIST SP 800-38D
Digital Signatures	ED25519	256-bit	RFC 8032
Password Hashing	bcrypt	Cost 12	OpenBSD
Key Management	AWS KMS	256-bit AES	FIPS 140-2 Level 2
Transport Security	TLS 1.3	256-bit	RFC 8446

Certificate Transparency Log

CT Log Implementation: The system maintains a Certificate Transparency-inspired append-only log for all data modifications. This provides an additional layer of integrity verification beyond the standard audit trail, enabling third-party verifiability of the complete data history.

Integrity Verification Summary

50	FAIL	6
HASHED ENTRIES	CHAIN INTEGRITY	CRYPTO ALGORITHMS

9 Data Classification Summary

Data classification ensures appropriate handling controls are applied based on sensitivity level. The system implements four classification tiers aligned with ISO 27001 and FDA data integrity guidelines.

Classification Levels

LEVEL	CLASSIFICATION	DESCRIPTION	ENCRYPTION	ACCESS LOGGING	MFA REQUIRED	ACCESS ROLES
1	**Public**	Information intended for public release	No	No	No	Viewer, QaUser, QaManager, Auditor, Admin
2	**Internal**	Internal business information	No	✓ COMPLIANT	No	QaUser, QaManager, Auditor, Admin
3	**Confidential**	Sensitive business and personal data	✓ COMPLIANT	✓ COMPLIANT	✓ COMPLIANT	QaManager, Auditor, Admin
4	**Restricted**	Highly sensitive PHI/PII, trade secrets	✓ COMPLIANT	✓ COMPLIANT	✓ COMPLIANT	Admin

PII/PHI Handling Summary

CONTROL	STATUS	IMPLEMENTATION
PII Identification	✓ COMPLIANT	Automated PII detection in data entry fields; classification tagging
PHI Protection	✓ COMPLIANT	AES-256-GCM encryption for Confidential/Restricted data; field-level masking in logs
Access Control	✓ COMPLIANT	Role-based access per classification level; need-to-know for Restricted
Audit Logging	✓ COMPLIANT	All access to Confidential+ data logged in audit trail
Data Minimization	⚠ PARTIAL	Retention policies defined; automated purging implementation pending
Cross-Border Transfer	⚠ PARTIAL	Data residency controls at tenant level; SCCs pending for EU transfers

Note: No explicit classification assignments recorded. Default classification policies apply based on data type and sensitivity rules.

9a Lab Results & OOS Detection

2185	231	4
TOTAL LAB RESULTS	OOS INVESTIGATIONS	SPEC LIMITS DEFINED

Results by Status

STATUS	COUNT
pending_review	1954
oos_investigation	231

OOS investigations initiated: **231**. All OOS events are tracked with full audit trail and require documented root cause analysis.

9b Equipment Qualification

288	1
TOTAL EQUIPMENT	CALIBRATIONS

Equipment by Qualification Status

QUALIFICATION STATUS	COUNT
fully qualified	2
iq complete	7
requalification required	1
unqualified	277
oq complete	1

9c Data Governance

155	3
GOVERNANCE POLICIES	ACTIVE DATA OWNERS

Policies by Status

STATUS	COUNT
draft	153
active	2

9d Audit Trail Review

3	0
REVIEWS COMPLETED	ANOMALIES DETECTED

Reviews by Status

STATUS	COUNT
completed	3

9e Data Lifecycle Management

3
LIFECYCLE RECORDS

Records by Lifecycle Stage

STAGE	COUNT
approval	1
review	2

9f DI Risk Assessment

6
RISK ITEMS

8
FDA RISK THRESHOLDS

Risk Items by Level

RISK LEVEL	COUNT
high	5
low	1

Deviation & CAPA Summary

All findings identified in this report are tracked through the deviation and CAPA management system per ICH Q10 and FDA 21 CFR 211.192.

0
TOTAL DEVIATIONS

0
OPEN DEVIATIONS

0
TOTAL CAPAS

0
OPEN CAPAS

Report Findings Linked to CAPA

FINDING	SEVERITY	CAPA ID	CAPA STATUS
Unsigned records detected: 50 entries require signatures but remain unsigned.	MEDIUM	CAPA-SIG-001	Open
Audit trail hash chain discontinuity detected. Potential data integrity issue.	CRITICAL	CAPA-AUDIT-001	Open
5 data entries with critical risk scores (>75) require investigation.	HIGH	CAPA-RISK-001	Open
22 suspicious audit events (DELETE actions or login failures) detected.	MEDIUM	CAPA-SEC-001	Under Review

CAPA Process: All findings with severity Medium or above are assigned a CAPA per ICH Q10. CAPAs are tracked to closure with effectiveness verification. Root cause analysis uses Ishikawa (fishbone) methodology.

10 Appendix — Methodology

Compliance Score Calculation

Nessa calculates compliance scores using a weighted assessment across multiple dimensions:

DIMENSION	WEIGHT	METHODOLOGY
Audit Trail Completeness	20%	Ratio of hashed/attributed events to total events
Electronic Signature Coverage	15%	Ratio of signed entries to entries requiring signatures
Data Integrity Hashing	15%	Percentage of entries with valid SHA-256 hashes
Hash Chain Integrity	15%	Binary: chain intact or broken
Access Control Enforcement	10%	RBAC implementation coverage
Risk Score Distribution	10%	Weighted average of entry risk scores (inverse)
ALCOA+ Principle Coverage	10%	Average score across 9 ALCOA+ principles
System Validation Status	5%	Automated test coverage and validation evidence

Cryptographic Algorithms

ALGORITHM	PURPOSE	STANDARD	IMPLEMENTATION
AES-256-GCM	Field-level encryption of sensitive data	NIST SP 800-38D	Rust `aes-gcm 0.10` crate, 96-bit nonces
ED25519	Digital signatures for electronic records	RFC 8032	Rust `ed25519-dalek 2.1`, 32-byte keys
SHA-256	Data integrity hashing, Merkle trees, audit chain	FIPS 180-4	Standard library, used for all hash operations
bcrypt	Password hashing	OpenBSD standard	Cost factor 12, per-password unique salt
AWS KMS	Key management and envelope encryption	FIPS 140-2 Level 2	AWS SDK, data key caching

Audit Trail Immutability

The audit trail is protected by multiple mechanisms:

- PostgreSQL trigger (`audit_log_immutability`) prevents UPDATE and DELETE operations
- Sequential hash chain links each entry to its predecessor
- Entry hashes include timestamp, user ID, action, and payload
- Database-level row security policies enforce tenant isolation
- Write-Ahead Logging (WAL) provides point-in-time recovery

NTP Time Source Verification

All timestamps are verified against NTP time sources to ensure temporal integrity. The system monitors clock drift and flags entries where the server time deviates more than 5 seconds from authoritative NTP sources. This ensures compliance with 21 CFR 11.10(e) requirements for time-stamped audit trails.

Report Generation

This report was generated automatically by Nessa's compliance reporting engine. All data was queried directly from the production database at the time of generation. No manual modifications were made to the data presented.

Document Change History

VERSION	DATE	AUTHOR	DESCRIPTION
1.0	2026-04-08	Nessa (Automated)	Initial automated compliance assessment

Report Review & Approval

This report must be reviewed and approved by authorized quality personnel before submission to regulatory authorities. Electronic signatures below constitute legally binding approval per 21 CFR Part 11.

ROLE	NAME	SIGNATURE	DATE	MEANING
Prepared by	_____	_____	____/____/_____	Authorship
Reviewed by (QA)	_____	_____	____/____/_____	Review
Approved by (QA Director)	_____	_____	____/____/_____	Approval

Signature meanings per 21 CFR 11.50: Authorship = "I generated this report", Review = "I have reviewed the findings and data", Approval = "I approve this report for regulatory submission"

End of Report

Report ID: FDA-DEFAULT--MNPUY6BY | Document Control: BEFB4F323F11EF1A
Generated by Nessa — Clinivion Pharmaceutical Data Integrity Platform
Retain for minimum 15 years per 21 CFR Part 11 requirements