COMMERCIAL IN CONFIDENCE

SDPF Style 10 Specification

Clinical Trial Data Management System

Specification ID	PHARMALOGIC-CTDMS-v1.0.0
Style	10 — Compliance-Driven
Version	1.1
Date	14 March 2026
Author	Hamza Abdullah, SDPF
Client	PharmaLogic Systems Ltd
Classification	Commercial in Confidence
Governing Spec	SDPF Language Specification v1.3.1

S-00 Phase 0 — Problem Definition

P0-1: Problem Observation Record

Observation Date	17 March 2026
Observer	Hamza Abdullah
Observed System	PharmaLogic CTDMS AI-assisted development process
Observation Method	Direct observation of 14 consecutive AI-assisted development sessions, January–February 2026

Observed Metrics

Metric	Observed Value
Avg correction cycles per feature	4.2
Number of sessions observed	14
AI-generated functions reviewed	40
Functions with REQ-ID trace	0 of 40
CTDMS releases in past 12 months	12
Releases with compliant audit trail	0 of 12
AI-generated specifications reviewed	9
Technical facts incorrect at implementation	7 of 31 (22.6%)
Requirement changes without impact assessment	23 in 6 months

P0-2: Five Failure Mode Assessment

Failure Mode	Status	Evidence
FM-1: Requirements only in someone's head	CONFIRMED	47-word avg Jira tickets, zero formal input contracts
FM-2: Tests written after code	CONFIRMED	11 of 14 sessions: tests written after AI output accepted
FM-3: Changes without consequence tracking	CONFIRMED	23 undocumented changes, 8 causing silent inconsistencies
FM-4: Code without traceable justification	CONFIRMED	3 of 40 functions untraced to any requirement
FM-5: Technical facts unverified	CONFIRMED	7 of 31 technical facts wrong at implementation

P0-3: Validated Problem Statement

Constructed using SDPF LSS DMAIC methodology. Four-component statement with four validation tests.

Component	Statement	Validation
Current State	The CTDMS AI-assisted development process produces an average of 4.2 correction cycles per feature before developer acceptance. Zero CTDMS releases in the past 12 months carry a traceable audit trail connecting AI-generated code to the regulatory clauses the code is required to satisfy.	T-1 Observable: PASS
Desired State	Zero correction cycles on first AI submission for CTDMS features. Every CTDMS release accompanied by a complete, signed, tamper-evident audit trail tracing every AI-generated function to its requirement and to the regulatory clause that requirement satisfies.	T-2 Bounded: PASS
Gap	4.2 correction cycles per feature above the zero target. 12 consecutive releases without a compliant audit trail against a target of one per release.	T-3 Cause-Free: PASS
Impact	USD 1.4M per year in AI-assisted development rework labour. 14-week regulatory submission preparation cycle per release. Eleven major findings in the most recent mock FDA inspection, all attributable to the absence of a compliant audit trail. Material risk of FDA Warning Letter at Q4 2026 inspection, with average remediation cost of USD 4–8M.	T-4 Solution-Free: PASS

Validated Problem Statement (P0-5)

> *"The CTDMS AI-assisted development process produces an average of 4.2 correction cycles per feature and zero compliant audit trail artefacts per release, against targets of zero correction cycles and one complete signed audit trail per release, resulting in USD 1.4M per year in rework, a 14-week regulatory submission overhead, eleven major mock inspection findings, and material risk of FDA Warning Letter at Q4 2026 inspection."*

Validation Test Results:

✓ T-1 Observable: PASS

✓ T-2 Bounded: PASS

✓ T-3 Cause-Free: PASS

✓ T-4 Solution-Free: PASS

P0-4: Problem Owner

Role	Name	Accountability
Problem Owner	Dr Sarah Chen, VP Regulatory Affairs	Accountable for closing the gap. Authority to approve S-11 regulatory mapping.
Technical Lead	T. Okonkwo, Lead Developer	Available for TVG execution. Technical support.
Executive Sponsor	Margaret Whitfield, CEO	Authorised engagement resources.

P0-5: Phase 0 Gate

Field	Value
Phase 0 Completion	Confirmed
Phase 1 Authorisation	APPROVED
Date	19 March 2026
Verifying Entity	Hamza Abdullah, SDPF

S-01 Style Declaration

Field	Value
Specification ID	PHARMALOGIC-CTDMS-v1.0.0
Style ID	10
Style Name	Compliance-Driven
Version	1.1
Stage	TSP_DRAFT — corrections applied, TVG re-execution required
Governing Specification	SDPF Language Specification v1.3.1
Lock Timestamp	PENDING — TVG re-execution required
REQ-ID Prefix	R-
TEST-ID Prefix	T-

Revision History

Version	Date	Description	Author
0.1 Draft	26 March 2026	Initial draft for RA review	H. Abdullah
0.2 Draft	28 March 2026	Updated S-11 per RA feedback	H. Abdullah
1.0 LOCKED	2 April 2026	Specification locked, all TVG entries PASS	H. Abdullah
1.1 DRAFT	26 April 2026	Corrections applied per external review: FDA endpoint, e-signatures (R-009), RBAC (R-010), backup/DR (R-011), 7-day AE window, ALCOA+ diff, session controls, key rotation, trial completion trigger. TVG re-execution pending.	H. Abdullah

Style Selection Justification (SDPF §11.2)

Condition	Evaluation	Result
Hardware constraints are the primary design driver	No — software-only system	Skip
System is regulated, compliance-driven, or security-critical	YES — 21 CFR Part 11, ICH E6(R2), FDA 21 CFR 312	Style 10
AI assistance will be used	Conditional — Style 4 considered	Not first match

Condition	Evaluation	Result
System requires formal verification evidence	Covered by Style 10	—

Conclusion: Style 10 is selected. The system operates in a regulated pharmaceutical environment and is subject to FDA inspection under 21 CFR Part 11.

Style 10 Mandatory Sections

Section	Requirement
S-11	Regulatory Mapping — every CRITICAL requirement maps to a named regulatory clause
S-12	Audit Evidence Requirements — evidence format, retention, signing specified
S-13	Compliance Verification Procedure — inspection readiness checklist defined

AI Framing Declaration

Per Style 10 — Compliance-Driven AI framing requirement, the AI executor for this specification shall be framed as follows when this specification is exported as a prompt (PROMPT-2):

> *You are an expert compliance engineer implementing a regulated clinical trial data management system under 21 CFR Part 11, ICH E6(R2), and FDA 21 CFR 312. You shall annotate every generated function with its REQ-ID and the regulatory clause that requirement satisfies. You shall include audit trail generation exactly as specified in PR-01 for every data operation. You shall not add any behaviour not defined in this specification. Every implementation artefact must be traceable to a named requirement and a named regulatory clause.*

AI Framing Property	Value
Role	Expert compliance engineer
REQ-ID annotation	Every function annotated with REQ-ID and regulatory clause mapping
Audit trail	Audit trail generation included as specified in PR-01 for every data operation
Scope constraint	No behaviour added beyond what is defined in this specification
Style authority	SDPF Language Specification v1.3.1, Section 11.3, Style 10

S-02 Style Context

System Clinical Trial Data Management System (CTDMS)

Organization PharmaLogic Systems Ltd

Domain Phase III Clinical Trials · Drug Safety Reporting

Markets EU and US

Regulatory Frameworks Governing

Framework	Scope
21 CFR Part 11	Electronic records, electronic signatures, audit trails
ICH E6(R2)	Good clinical practice — trial data integrity
FDA 21 CFR 312	IND (Investigational New Drug) safety reporting

System Boundary

In Scope:

- Subject Visit Record management
- Adverse Event reporting and FDA IND submission
- Audit trail generation and retention
- Electronic signature authentication

Out of Scope:

- Trial protocol design
- Patient recruitment systems
- Drug dispensing logistics
- Regulatory submission preparation (beyond evidence package)

Problem Statement Reference: See S-00 P0-5 above.

S-03 External Contract

Field	Value
Interface Type	REST HTTP API (FastAPI)
Data Serialisation Format	JSON (application/json)
Version Identifier	v1.0.0
Protocol	HTTPS, TLS 1.3 minimum
Problem Boundary Reference	PHARMALOGIC-CTDMS-v1.0.0 / S-02 System Boundary

Regulatory Frameworks (Input Contract Reference)

Framework	Edition
21 CFR Part 11	Current
ICH E6(R2)	Second Revision
FDA 21 CFR 312	Current

S-04 Input Contract

Field	Specification
Format	SDPF specification document (this document)
Version	v1.0.0
REQ-ID Range	R-001 through R-011
Style	10 — Compliance-Driven

Valid Input Operations — Field Definitions (IC-1 through IC-4)

Operation	Field	Type	Required	Nullable	Constraints
Create Subject Visit Record	record_id	String	Yes	No	UUID format
	subject_id	String	Yes	No	Non-null string
	operator_id	String	Yes	No	Non-null string

Operation	Field	Type	Required	Nullable	Constraints
	timestamp	String	Yes	No	ISO 8601 UTC
	payload	Object	Yes	No	Non-null JSON object
Read Subject Visit Record	record_id	String	Yes	No	UUID format
Update Subject Visit Record	record_id	String	Yes	No	UUID format
	operator_id	String	Yes	No	Non-null string
	timestamp	String	Yes	No	ISO 8601 UTC
	prior_hash	String	Yes	No	SHA-256 hex string
	new_payload	Object	Yes	No	Non-null JSON object
Delete Subject Visit Record	record_id	String	Yes	No	UUID format
	operator_id	String	Yes	No	Non-null string
	timestamp	String	Yes	No	ISO 8601 UTC
Submit Adverse Event	ae_id	String	Yes	No	UUID format
	subject_id	String	Yes	No	Non-null string
	awareness_date	String	Yes	No	ISO 8601 date
	event_data	Object	Yes	No	Non-null JSON object
Authenticate Operator	operator_id	String	Yes	No	Non-null string
	mfa_token	String	Yes	No	TOTP 6-digit integer string
Sign Record (Electronic Signature)	record_id	String	Yes	No	UUID format
	operator_id	String	Yes	No	Non-null string; must match authenticated session
	printed_name	String	Yes	No	Full legal name; non-null string
	signature_meaning	String	Yes	No	One of: AUTHORSHIP, REVIEW, APPROVAL
	timestamp	String	Yes	No	ISO 8601 UTC; server-generated
Declare Trial Completion	trial_id	String	Yes	No	Non-null string
	operator_id	String	Yes	No	ADMINISTRATOR role required
	completion_date	String	Yes	No	ISO 8601 UTC date
	declaration_signature	Object	Yes	No	§11.50-compliant e-signature object per PR-08

S-05 Processing Rules

All processing rules are SHALL statements. Each carries a priority tag per REQ-SYNTAX-1.

PR-01: Audit Trail Generation

PR-01: [CRITICAL] The system SHALL generate a cryptographically signed audit entry for every create, read, update, and delete operation on Subject Visit Records.

PR-01.1: [CRITICAL] The audit entry SHALL capture the operator identity of the user who performed the operation.

PR-01.2: [CRITICAL] The audit entry SHALL capture the timestamp of the operation in UTC, formatted as ISO 8601.

PR-01.3: [CRITICAL] The audit entry SHALL capture the operation type: one of CREATE, READ, UPDATE, or DELETE.

PR-01.4: [CRITICAL] The audit entry SHALL capture the record identifier of the Subject Visit Record affected.

PR-01.5: [CRITICAL] The audit entry SHALL capture the prior value hash of the record before the operation.

PR-01.6: [CRITICAL] The audit entry SHALL capture the new value hash of the record after the operation.

PR-01.7: [CRITICAL] The audit entry SHALL be signed with HMAC-SHA256 using the current provenance key.

PR-01.8: [CRITICAL] The audit entry SHALL store the human-readable field-level diff of the Subject Visit Record, enabling complete reconstruction of what changed per ALCOA+ completeness principles under 21 CFR §11.10(e).

PR-02: Audit Record Immutability

PR-02: [CRITICAL] Audit entries SHALL be immutable after creation.

PR-02.1: [CRITICAL] No update operation SHALL be permitted on any audit entry.

PR-02.2: [CRITICAL] No delete operation SHALL be permitted on any audit entry.

PR-02.3: [CRITICAL] Attempts to modify audit records SHALL be rejected with HTTP 403 and logged.

PR-03: Multi-Factor Authentication and Session Control

PR-03: [CRITICAL] The system SHALL authenticate every operator using multi-factor authentication before permitting any write operation on trial data.

PR-03.1: [CRITICAL] Authentication events SHALL be recorded in the audit log.

PR-03.2: [REQUIRED] Session tokens SHALL expire after 30 minutes of inactivity.

PR-03.3: [REQUIRED] Explicit operator logout SHALL invalidate the session token immediately and be recorded in the audit log.

PR-03.4: [REQUIRED] Browser or client close events SHALL invalidate the session token server-side within 60 seconds.

PR-03.5: [REQUIRED] Concurrent sessions for the same operator identity SHALL be limited to one active session at any time. A new login SHALL invalidate any existing session for that operator.

PR-04: Adverse Event Reporting — Expedited Safety Reports

PR-04: [CRITICAL] The system SHALL classify every adverse event by severity before submission and apply the correct reporting window per 21 CFR §312.32(c).

PR-04.1: [CRITICAL] Fatal or life-threatening unexpected adverse experiences SHALL be submitted to the FDA ESG IND safety reporting endpoint within 7 calendar days of awareness, per 21 CFR §312.32(c)(1). An initial brief report is sufficient; a follow-up within 15 days is then required.

PR-04.2: [CRITICAL] All other serious and unexpected adverse experiences SHALL be submitted to the FDA ESG IND safety reporting endpoint within 15 calendar days of awareness, per 21 CFR §312.32(c)(2).

PR-04.3: [CRITICAL] All submissions SHALL conform to the E2B R2 XML schema as verified in TVG-08.

PR-04.4: [CRITICAL] Submission timestamp SHALL be recorded for every report.

PR-04.5: [CRITICAL] FDA ESG acknowledgement receipt SHALL be stored and auditable.

PR-04.6: [CRITICAL] The system SHALL prevent submission of AE reports that fail E2B R2 schema validation. Validation failures SHALL be logged and escalated.

PR-05: Verification Closure

PR-05: [CRITICAL] The system SHALL produce a Verification Closure Record for every release.

PR-05.1: [CRITICAL] The closure record SHALL be signed with HMAC-SHA256 using the current provenance key.

PR-05.2: [CRITICAL] The closure record SHALL contain: Specification version, Verification timestamp, CLOSURE STATUS.

PR-06: Data Encryption and Key Management

PR-06: [REQUIRED] Subject data exports SHALL be encrypted at rest using AES-256.

PR-06.1: [REQUIRED] Data in transit SHALL use TLS 1.3 minimum.

PR-06.2: [REQUIRED] AES-256 encryption key rotation SHALL occur on a 90-day cycle.

PR-06.3: [REQUIRED] The HMAC-SHA256 provenance signing key SHALL be rotated on a 90-day cycle. Key versions SHALL be tracked and prior key versions retained for re-verification of historical evidence packages.

PR-07: Audit Log Retention

PR-07: [REQUIRED] The system SHALL retain all audit logs for a minimum of 15 years from trial completion date per 21 CFR §312.62.

PR-07.1: [REQUIRED] Trial completion SHALL be defined as the date on which the final database lock is recorded in the system by an authorised administrator.

PR-07.2: [REQUIRED] The trial completion date SHALL be recorded as an immutable audit entry at the time of database lock, capturing the authorised administrator identity, timestamp, and completion declaration.

PR-07.3: [REQUIRED] The 15-year retention clock SHALL start from the trial completion date recorded per PR-07.2. The system SHALL enforce this retention period automatically and prevent deletion of audit records within the retention window.

PR-08: Electronic Signature

PR-08: [CRITICAL] The system SHALL capture a §11.50-compliant electronic signature for every data-locking operation on Subject Visit Records and Adverse Event reports.

PR-08.1: [CRITICAL] Each electronic signature SHALL capture the printed name of the signing operator.

PR-08.2: [CRITICAL] Each electronic signature SHALL capture the date and time of signing in UTC, formatted as ISO 8601.

PR-08.3: [CRITICAL] Each electronic signature SHALL capture the meaning of the signature, which SHALL be one of: AUTHORSHIP, REVIEW, or APPROVAL.

PR-08.4: [CRITICAL] Each electronic signature SHALL be non-repudiable, linking the signature record to the operator identity verified by PR-03 MFA and to the HMAC-SHA256 provenance key.

PR-08.5: [CRITICAL] Electronic signature events SHALL be recorded in the audit trail per PR-01.

PR-09: Role-Based Access Control

PR-09: [CRITICAL] The system SHALL enforce role-based access control (RBAC) with least-privilege principles per 21 CFR §11.10(d) and ICH E6(R2) §5.5.2.

PR-09.1: [CRITICAL] The system SHALL define the following roles: DATA_ENTRY, DATA_REVIEWER, DATA_MANAGER, ADMINISTRATOR, AUDITOR.

PR-09.2: [CRITICAL] DATA_ENTRY operators SHALL be permitted to create and update Subject Visit Records and submit Adverse Events only. Read access to own submissions only.

PR-09.3: [CRITICAL] DATA_REVIEWER operators SHALL be permitted to read all records and approve data. No create, update, or delete permissions.

PR-09.4: [CRITICAL] DATA_MANAGER operators SHALL be permitted all DATA_ENTRY and DATA_REVIEWER permissions plus database lock initiation.

PR-09.5: [CRITICAL] ADMINISTRATOR operators SHALL be permitted role assignment, system configuration, and trial completion declaration. No direct trial data access.

PR-09.6: [CRITICAL] AUDITOR operators SHALL be permitted read-only access to audit trails only. No access to Subject Visit Record payload data.

PR-09.7: [CRITICAL] Role assignments SHALL be recorded in the audit trail. Role changes SHALL require ADMINISTRATOR authority and electronic signature per PR-08.

PR-10: Backup and Disaster Recovery

PR-10: [REQUIRED] The system SHALL maintain a complete and accurate backup of all trial data and audit logs per 21 CFR §11.10(c).

PR-10.1: [REQUIRED] Full backups SHALL be performed daily. Incremental backups SHALL be performed every 6 hours.

PR-10.2: [REQUIRED] Backups SHALL be stored in a geographically separate location from the primary system.

PR-10.3: [REQUIRED] Backup integrity SHALL be verified by checksum on every backup completion. Failed backup verification SHALL trigger immediate escalation.

PR-10.4: [REQUIRED] Recovery time objective (RTO) SHALL be 4 hours maximum from declared disaster event.

PR-10.5: [REQUIRED] Recovery point objective (RPO) SHALL be 6 hours maximum, consistent with incremental backup frequency.

PR-10.6: [REQUIRED] Disaster recovery SHALL be tested at minimum annually. Test results SHALL be documented and retained as part of the audit evidence.

PR-11: Electronic Signature Non-Repudiation Link

PR-11: [CRITICAL] The system SHALL ensure that electronic signatures cannot be excised, copied, or transferred to falsify records, per 21 CFR §11.70.

PR-11.1: [CRITICAL] Each electronic signature record SHALL contain an embedded reference to the signed record identifier such that the signature is inseparable from the record it signs.

PR-11.2: [CRITICAL] Any attempt to apply an existing signature to a different record SHALL be rejected with HTTP 403 and logged.

S-06 Output Guarantees

OG-A: API Success Response Shapes

Per OG-1 and OG-2, the complete structure of every success response and its HTTP status code are defined below for each input operation declared in S-04.

Operation	HTTP Status	Success Response Structure
Create Subject Visit Record	201 Created	{"data": {"record_id": string, "subject_id": string, "operator_id": string, "timestamp": ISO8601, "audit_entry_id": string}, "status": "CREATED"}
Read Subject Visit Record	200 OK	{"data": {"record_id": string, "subject_id": string, "payload": object, "created_at": ISO8601, "audit_entry_id": string}, "status": "OK"}
Update Subject Visit Record	200 OK	{"data": {"record_id": string, "operator_id": string, "timestamp": ISO8601, "prior_hash": string, "new_hash": string, "audit_entry_id": string}, "status": "UPDATED"}
Delete Subject Visit Record	200 OK	{"data": {"record_id": string, "deleted_at": ISO8601, "operator_id": string, "audit_entry_id": string}, "status": "DELETED"}
Submit Adverse Event	202 Accepted	{"data": {"ae_id": string, "submission_timestamp": ISO8601, "fda_endpoint": string, "status": "SUBMITTED"}, "status": "ACCEPTED"}
Authenticate Operator	200 OK	{"data": {"operator_id": string, "session_token": string, "expires_at": ISO8601, "audit_entry_id": string}, "status": "AUTHENTICATED"}
Sign Record	200 OK	{"data": {"signature_id": string, "record_id": string, "operator_id": string, "printed_name": string, "meaning": string, "timestamp": ISO8601, "audit_entry_id": string}, "status": "SIGNED"}
Declare Trial Completion	200 OK	{"data": {"trial_id": string, "completion_date": ISO8601, "declared_by": string, "retention_expiry": ISO8601, "audit_entry_id": string}, "status": "TRIAL_COMPLETE"}

OG-01: Traceability Guarantee

OG-01: [CRITICAL] Every requirement SHALL be traceable to a test case.

OG-01.1: [CRITICAL] Every test case SHALL carry a REQ-ID reference.

OG-01.2: [CRITICAL] Every implementation function SHALL carry a REQ-ID annotation.

OG-02: Evidence Package Guarantee

OG-02: [CRITICAL] Every release SHALL produce a Level 3 conforming evidence package.

OG-02.1: [CRITICAL] The evidence package SHALL contain: specification_id, style, stage, problem_statement, regulatory_frameworks, requirements_count, traceability_matrix, verification_timestamp, closure_status, provenance_signature.

OG-03: Regulatory Mapping Guarantee

OG-03: [CRITICAL] Every CRITICAL requirement SHALL map to at least one named regulatory clause.

OG-03.1: [REQUIRED] The mapping SHALL be approved by the Regulatory Affairs team.

S-07 Exception Handling

EH-ID	Condition	HTTP Code	Response Shape	Recovery / Escalation
EH-01	Unauthenticated write attempt	401 Unauthorized	{"error":"UNAUTHENTICATED","message":"Authentication required before write operations."}	Log attempt in audit trail; return 401; no data written.
EH-02	Attempt to modify or delete an audit record	403 Forbidden	{"error":"AUDIT_IMMUTABLE","message":"Audit records are immutable."}	[CRITICAL] Reject and log. Escalate to security team if repeated within session.
EH-03	TVG entry failure at lock time	N/A (pre-lock gate)	Blocking error surfaced by tool	Specification remains in TSP_DRAFT. Update spec or environment. Retry all TVG entries.
EH-04	Verification gate check failure	N/A (post-code gate)	CLOSURE STATUS = INCOMPLETE	[CRITICAL] Evidence export blocked. Resolve failed VER checks before re-running gate.
EH-05	Adverse event submission timeout	503 Service Unavailable	{"error":"FDA_ENDPOINT_TIMEOUT","message":"FDA IND endpoint did not respond."}	[CRITICAL] Retry with exponential backoff. Alert operator. Log all retry attempts.
EH-06	MFA token invalid or expired	401 Unauthorized	{"error":"MFA_INVALID","message":"MFA token invalid or expired."}	Reject write operation. Require re-authentication. Log event.
EH-07	E2B R2 schema validation failure on AE submission	422 Unprocessable Entity	{"error":"AE_SCHEMA_INVALID","message":"AE report failed E2B R2 schema validation.","field": string|null}	[CRITICAL] Reject submission. Log validation failure. Escalate to Data Manager. Do not submit invalid report to FDA ESG.
EH-08	Concurrent session detected on login	409 Conflict	{"error":"SESSION_CONFLICT","message": "An active session exists for this operator. Existing session has been invalidated."}	Invalidate prior session. Proceed with new session. Log both events.
EH-09	Electronic signature attempted by unauthorised role	403 Forbidden	{"error":"SIGNATURE_ROLE_DENIED","message":"Operator role does not permit signing this record type."}	[CRITICAL] Reject signature. Log attempt with operator_id and record_id. Escalate if repeated.

EH-ID	Condition	HTTP Code	Response Shape	Recovery / Escalation
EH-10	Backup verification checksum failure	N/A (background process)	{"error":"BACKUP_CHECKSUM_FAILED","message":"Backup integrity verification failed."}	[CRITICAL] Halt backup rotation. Alert ADMINISTRATOR immediately. Initiate emergency backup procedure. Do not overwrite failed backup until investigation complete.
EH-11	Unauthorised role assignment attempt	403 Forbidden	{"error":"RBAC_ASSIGNMENT_DENIED","message":"Role assignment requires ADMINISTRATOR authority."}	Reject assignment. Log attempt. Escalate to security team if repeated within session.

S-08 Technical Verification Gate (TVG)

> *CORE PRINCIPLE II — Facts Before Execution: No implementation begins until every asserted technical fact in the specification is verified against live output. All entries below must PASS before this specification is locked. HALT rules are non-negotiable: a conforming practitioner treats any failure as a specification problem, not a build problem.*

TVG-01: Python Runtime

Field	Value
Tool / Asset	python
Asserted Value	3.11.9
Verification Command	python --version
Pass Condition	Output contains "Python 3.11.9"
HALT	**Do NOT proceed under any Python version other than 3.11.9. Update the environment or correct this specification entry before any implementation begins.**
Result	**PASS**

TVG-02: FastAPI

Field	Value
Tool / Asset	fastapi
Asserted Value	0.111.0
Verification Command	pip show fastapi | grep Version
Pass Condition	Output contains "Version: 0.111.0"
HALT	**Do NOT proceed if FastAPI version is not 0.111.0. Install the correct version or update this specification entry. No implementation begins on a version mismatch.**
Result	**PASS**

TVG-03: SQLAlchemy

Field	Value
Tool / Asset	sqlalchemy
Asserted Value	2.0.30
Verification Command	pip show sqlalchemy | grep Version
Pass Condition	Output contains "Version: 2.0.30"
HALT	**Do NOT proceed if SQLAlchemy version is not 2.0.30. Install the correct version or update this specification entry before implementation.**
Result	**PASS**

TVG-04: FDA ESG IND Safety Reporting Endpoint

Field	Value
Tool / Asset	https://esg.fda.gov/gateway/submission
Asserted Value	HTTP 200 or 302 response; ESG gateway reachable
Verification Command	curl -s -o /dev/null -w "%{http_code}" https://esg.fda.gov/gateway/submission
Pass Condition	Output = "200" or "302" (ESG gateway redirect to submission portal)
HALT	**Do NOT proceed if the FDA ESG gateway is not reachable. This is the IND safety report submission endpoint under 21 CFR §312.32(c), not a query API. Verify submission schema compatibility separately via TVG-08 before implementing AE submission logic.**
Result	**PASS**

TVG-08: FDA ESG E2B R2 Submission Schema

Field	Value
Tool / Asset	E2B R2 XML schema file present at /etc/ctdms/fda_e2b_r2.xsd
Asserted Value	Schema file present and valid
Verification Command	xmllint --noout /etc/ctdms/fda_e2b_r2.xsd 2>&1 | grep -c "validates"
Pass Condition	Output >= 1
HALT	**Do NOT proceed without the validated E2B R2 schema. AE reports must conform to this schema for FDA ESG submission under §312.32(c). Schema must be obtained from FDA ESG documentation and placed at the asserted path before implementation begins.**
Result	**PASS**

TVG-09: Electronic Signature Library (pyhanko)

Field	Value
Tool / Asset	pyhanko
Asserted Value	0.21.0
Verification Command	pip show pyhanko | grep Version
Pass Condition	Output contains "Version: 0.21.0"
HALT	**Do NOT proceed if pyhanko version is not 0.21.0. This library is required for §11.50-compliant electronic signature capture. Install the correct version or update this specification entry before implementing electronic signature operations.**
Result	**PASS**

TVG-05: PostgreSQL

Field	Value
Tool / Asset	PostgreSQL
Asserted Value	16.3
Verification Command	psql --version
Pass Condition	Output contains "16.3"
HALT	**Do NOT proceed if PostgreSQL version is not 16.3. Upgrade the database instance or update this specification entry before implementation.**

Field	Value
Result	**PASS**

TVG-06: HMAC-SHA256 Provenance Signing Key

Field	Value
Tool / Asset	Environment variable PHARMALOGIC_PROV_KEY_2026
Asserted Value	Key present, length >= 64 characters (256-bit minimum)
Verification Command	printenv PHARMALOGIC_PROV_KEY_2026 | wc -c
Pass Condition	Output >= 64
HALT	**Do NOT proceed if PHARMALOGIC_PROV_KEY_2026 is not set or returns fewer than 64 characters. Provision the key in the target environment before any signed artefact is generated.**
Result	**PASS**

TVG-07: TLS Version

Field	Value
Tool / Asset	TLS protocol on localhost:443
Asserted Value	1.3
Verification Command	openssl s_client -connect localhost:443 2>&1 | grep "Protocol"
Pass Condition	Output contains "TLSv1.3"
HALT	**Do NOT proceed if TLS version is not 1.3. Configure the server to enforce TLS 1.3 minimum before any data-in-transit guarantee is asserted in implementation.**
Result	**PASS**

S-09 Verification Requirements

All test cases below shall pass for CLOSURE STATUS = COMPLETE. Each test carries a REQ-ID trace per OG-01.1.

Eleven Structural Invariant Checks

Check ID	Name	REQ-ID Trace	Pass Condition
VER-1	spec_exists	R-005	Specification present at SPEC_LOCKED
VER-2	style_defined	R-005	Style 10 declared in S-01
VER-3	tests_exist	OG-01	31 test cases generated from locked specification
VER-4	tests_locked	OG-01	Tests frozen before code generation begins
VER-5	implementation_exists	OG-01	Implementation generated from locked tests and spec
VER-6	traceability_complete	OG-01.1	All 31 REQ-IDs present in traceability matrix
VER-7	style_constraints_present	R-005	Style 10 keywords present: regulatory mapping, audit evidence, compliance

Check ID	Name	REQ-ID Trace	Pass Condition
VER-8	style_10_regulatory_mapping	OG-03	S-11 non-empty; all CRITICAL requirements carry regulatory clause mapping
VER-9	policy_engine_passed	R-005	No semantic violations flagged by policy engine
VER-10	ci_gate_ready	R-005	CI workflow generated and valid
VER-11	provenance_signing_ready	R-005	HMAC-SHA256 key configured; TVG-06 PASS confirmed

Functional Test Cases

TEST-ID	REQ-ID	Description	Pass Condition
T-001	R-001	Audit entry created on Subject Visit Record CREATE	Audit entry exists with operator_id, UTC timestamp, operation=CREATE, record_id, prior_hash=null, new_hash present; HMAC-SHA256 signature valid
T-002	R-001	Audit entry created on Subject Visit Record READ	Audit entry exists with operation=READ, all required fields present and signed
T-003	R-001	Audit entry created on Subject Visit Record UPDATE	Audit entry captures prior_hash and new_hash; signature valid
T-004	R-001	Audit entry created on Subject Visit Record DELETE	Audit entry exists with operation=DELETE; record logically deleted; signature valid
T-005	R-002	UPDATE attempt on audit record returns HTTP 403	Response status = 403; error code = AUDIT_IMMUTABLE; attempt logged in audit trail
T-006	R-002	DELETE attempt on audit record returns HTTP 403	Response status = 403; error code = AUDIT_IMMUTABLE; attempt logged in audit trail
T-007	R-003	Write operation rejected without MFA	Response status = 401; no data written; attempt logged
T-008	R-003	MFA authentication event recorded in audit log	Audit entry with operation=AUTH present after successful MFA; operator_id and timestamp captured
T-009	R-003	Session token expires after 30 minutes of inactivity	Token invalid after 30-minute inactivity window; subsequent request returns 401
T-010	R-004	AE report submitted within 15 calendar days of awareness_date	FDA endpoint receives POST within 15 days; submission_timestamp recorded; no submission > 15 days from awareness_date
T-011	R-004	FDA acknowledgement receipt stored and auditable	Receipt present in audit-queryable storage within 1 hour of submission
T-012	R-005	Verification Closure Record produced on release	VCR present with specification_version, verification_timestamp, and CLOSURE_STATUS fields
T-013	R-005	VCR signed with HMAC-SHA256 using PHARMALOGIC_PROV_KEY_2026	Signature valid; key ID = PL_PROV_2026_Q1
T-014	R-006	Subject data export encrypted at rest with AES-256	Export file passes AES-256 verification check; plaintext not readable without key
T-015	R-006	Data in transit uses TLS 1.3 minimum	Protocol inspector confirms TLSv1.3 on all API connections

TEST-ID	REQ-ID	Description	Pass Condition
T-016	R-006	Key rotation occurs on 90-day cycle	Key rotation log shows rotation event <= 90 days prior to test date
T-017	R-007	Audit logs retained for 15 years from trial completion	Retention policy configured to 15 years; policy document present and signed
T-018	R-007 PR-07.1	Trial completion defined by database lock event	System records immutable audit entry on database lock; trial completion date captured with ADMINISTRATOR identity and timestamp
T-019	R-009 PR-08	Electronic signature captures printed name, timestamp, meaning	Signed record contains printed_name, ISO 8601 UTC timestamp, and meaning from {AUTHORSHIP, REVIEW, APPROVAL}; all fields non-null
T-020	R-009 PR-08.4	Electronic signature is non-repudiable	Signature record contains embedded record_id reference; signature cannot be applied to a different record; attempt to reuse signature returns HTTP 403
T-021	R-009 PR-11	Signature inseparable from signed record	Attempt to excise or transfer signature to another record returns HTTP 403 and is logged
T-022	R-010 PR-09	RBAC enforces role permissions	DATA_ENTRY role cannot approve records; DATA_REVIEWER role cannot create records; AUDITOR role cannot access payload data; all violations return HTTP 403
T-023	R-010 PR-09.7	Role changes require ADMINISTRATOR authority and e-signature	Role assignment by non-ADMINISTRATOR returns HTTP 403; successful assignment recorded in audit trail with e-signature
T-024	R-011 PR-10	Daily full backup and 6-hour incremental backup executed	Backup log shows daily full backup and 6-hour incremental; timestamps within expected windows
T-025	R-011 PR-10.3	Backup integrity verified by checksum	Backup verification log shows checksum PASS for every backup; failed checksum triggers ADMINISTRATOR alert within 5 minutes
T-026	R-011 PR-10	RTO <= 4 hours from declared disaster	Disaster recovery test demonstrates system restoration within 4 hours; test results documented and signed
T-027	R-004 PR-04.1	7-day fatal/life-threatening AE submitted within 7 days	AE classified as fatal or life-threatening is submitted to FDA ESG within 7 calendar days of awareness_date; submission_timestamp - awareness_date <= 7 days
T-028	R-004 PR-04.3	AE submission conforms to E2B R2 schema	AE submission XML validates against E2B R2 schema file at /etc/ctdms/fda_e2b_r2.xsd; no validation errors
T-029	R-004 PR-04.6	Invalid E2B schema submission rejected	AE report failing schema validation returns HTTP 422; error code AE_SCHEMA_INVALID; submission not forwarded to FDA ESG; failure logged and escalated

TEST-ID	REQ-ID	Description	Pass Condition
T-030	PR-03.3 PR-03.4	Explicit logout and browser-close invalidate session	After logout, session token returns 401 on subsequent request; server-side session invalidated within 60 seconds of browser close event
T-031	PR-03.5	Concurrent session limit enforced	Second login for same operator invalidates first session; first session token returns 401 after second login

CLOSURE STATUS Values

Status	Meaning
INCOMPLETE	One or more VER checks or functional tests failed
COMPLETE	All 11 structural checks and all functional tests passed

S-10 Traceability Matrix

Format: REQ-ID → TEST-ID(s) → Implementation Artifact. Per TM-1: all CRITICAL requirements covered. Per TM-2: all REQUIRED requirements covered.

REQ-ID	Priority	Test ID(s)	Implementation Artifact
R-001	CRITICAL	T-001, T-002, T-003, T-004	audit_trail_service.generate_signed_entry()
R-002	CRITICAL	T-005, T-006	audit_trail_service.enforce_immutability()
R-003	CRITICAL	T-007, T-008, T-009	auth_service.mfa_authenticate()
R-004	CRITICAL	T-010, T-011	ae_reporting_service.submit_to_fda()
R-005	CRITICAL	T-012, T-013	vcr_service.generate_closure_record()
R-006	REQUIRED	T-014, T-015, T-016	encryption_service.encrypt_export() / tls_config
R-007	REQUIRED	T-017	retention_policy_service.configure_retention()
R-008	OPTIONAL	—	audit_report_service.generate_pdf_a3() (optional)
R-009	CRITICAL	T-019, T-020, T-021	esig_service.capture_electronic_signature()
R-010	CRITICAL	T-022, T-023	rbac_service.enforce_role_permissions()
R-011	REQUIRED	T-024, T-025, T-026	backup_service.execute_backup() / dr_service.restore()

Change Protocol

Classification	Definition	Action
BREAKING	Requirement removed or fundamentally altered	Full re-verification required from SPEC_LOCKED
SIGNIFICANT	Processing rule or output guarantee modified	Component re-verification required
MINOR	Typographical, formatting, or clarificatory	Review only; no re-verification required

Post-Lock Change Process

1. Change SHALL be classified before implementation
2. BREAKING changes require full re-verification from SPEC_LOCKED
3. SIGNIFICANT changes require component re-verification

4. MINOR changes require documentation update only

S-11 Regulatory Mapping

Style 10 mandatory section. Every CRITICAL requirement maps to at least one named regulatory clause (OG-03). Approved by Regulatory Affairs per OG-03.1.

R-001: Audit Trail Generation — CRUD Operations

REQ-ID	Priority	Requirement	Regulatory Mapping
R-001	**CRITICAL**	[CRITICAL] The system shall generate a cryptographically signed audit entry for every create, read, update, and delete operation on Subject Visit Records, capturing operator identity, timestamp (UTC, ISO 8601), operation type, record identifier, prior value hash, and new value hash.	21 CFR §11.10(e) ICH E6(R2) §5.5.3

R-002: Audit Record Immutability

REQ-ID	Priority	Requirement	Regulatory Mapping
R-002	**CRITICAL**	[CRITICAL] Audit entries shall be immutable after creation. No update or delete operation shall be permitted on any audit entry. Attempts shall be rejected with HTTP 403 and logged.	21 CFR §11.10(e) 21 CFR §11.10(k)

R-003: Multi-Factor Authentication

REQ-ID	Priority	Requirement	Regulatory Mapping
R-003	**CRITICAL**	[CRITICAL] The system shall authenticate every operator using multi-factor authentication before permitting any write operation on trial data. Authentication events shall be recorded in the audit log.	21 CFR §11.200(a) ICH E6(R2) §5.5.2

R-004: Adverse Event Reporting — 15-Day Window

REQ-ID	Priority	Requirement	Regulatory Mapping
R-004	**CRITICAL**	[CRITICAL] Every adverse event report shall be submitted to the FDA IND safety reporting endpoint within 15 calendar days of awareness. Submission timestamp and FDA acknowledgement receipt shall be stored and auditable.	21 CFR §312.32(c) ICH E6(R2) §4.11

R-005: Verification Closure Record

REQ-ID	Priority	Requirement	Regulatory Mapping
R-005	**CRITICAL**	[CRITICAL] The system shall produce a Verification Closure Record for every release, signed with HMAC-SHA256 using the current provenance key, containing the specification version, verification timestamp, and CLOSURE STATUS.	21 CFR §11.10(a) SDPF Principle III

R-006: Data Encryption

REQ-ID	Priority	Requirement	Regulatory Mapping
R-006	**REQUIRED**	[REQUIRED] Subject data exports shall be encrypted at rest using AES-256 and in transit using TLS 1.3 minimum. Key rotation shall occur on a 90-day cycle.	21 CFR §11.10(d) HIPAA §164.312

R-007: Audit Log Retention

REQ-ID	Priority	Requirement	Regulatory Mapping
R-007	**REQUIRED**	[REQUIRED] All audit logs shall be retained for a minimum of 15 years from trial completion date, in accordance with FDA inspection requirements.	21 CFR §312.62 ICH E6(R2) §8.1

R-008: Audit Summary Report (PDF/A-3)

REQ-ID	Priority	Requirement	Regulatory Mapping
R-008	**OPTIONAL**	[OPTIONAL] The system may generate a human-readable audit summary report in PDF/A-3 format suitable for direct submission to regulatory authorities.	21 CFR Part 11 (general)

R-009: Electronic Signature — §11.50 Compliance

REQ-ID	Priority	Requirement	Regulatory Mapping
R-009	**CRITICAL**	[CRITICAL] The system shall capture a §11.50-compliant electronic signature for every data-locking operation, including: printed name of the signer, date and time of signing in UTC ISO 8601, and meaning of the signature (AUTHORSHIP, REVIEW, or APPROVAL). Signatures shall be non-repudiable and inseparable from the signed record per 21 CFR §11.70.	21 CFR §11.50 21 CFR §11.70 ICH E6(R2) §5.5.2

R-010: Role-Based Access Control

REQ-ID	Priority	Requirement	Regulatory Mapping
R-010	**CRITICAL**	[CRITICAL] The system shall enforce role-based access control with least-privilege principles. Defined roles: DATA_ENTRY, DATA_REVIEWER, DATA_MANAGER, ADMINISTRATOR, AUDITOR. Each role shall have defined and enforced permissions. Role assignments shall be auditable and require ADMINISTRATOR authority with electronic signature.	21 CFR §11.10(d) ICH E6(R2) §5.5.2

R-011: Backup and Disaster Recovery

REQ-ID	Priority	Requirement	Regulatory Mapping
R-011	**REQUIRED**	[REQUIRED] The system shall maintain complete and accurate backups of all trial data and audit logs. Full backups daily; incremental every 6 hours. Geographically separated storage. RTO <= 4 hours. RPO <= 6 hours. Annual DR test with documented results.	21 CFR §11.10(c) 21 CFR §312.62

Output Guarantee Requirements — Regulatory Mapping

The following CRITICAL requirements from S-06 are mapped here per Style 10 semantic constraint: every CRITICAL requirement contains a regulatory mapping.

OG-01: Traceability Guarantee

REQ-ID	Priority	Requirement	Regulatory Mapping
OG-01	**CRITICAL**	[CRITICAL] Every requirement shall be traceable to a test case. Every test case shall carry a REQ-ID reference. Every implementation function shall carry a REQ-ID annotation.	21 CFR §11.10(e) SDPF Principle I SDPF §13 (Traceability Matrix TM-1 to TM-3)

OG-02: Evidence Package Guarantee

REQ-ID	Priority	Requirement	Regulatory Mapping
OG-02	**CRITICAL**	[CRITICAL] Every release shall produce a Level 3 conforming evidence package containing: specification_id, style, stage, problem_statement, regulatory_frameworks, requirements_count, traceability_matrix, verification_timestamp, closure_status, provenance_signature.	21 CFR §11.10(a) 21 CFR §312.62 SDPF Principle III SDPF §14 (Evidence Standard)

OG-03: Regulatory Mapping Guarantee

REQ-ID	Priority	Requirement	Regulatory Mapping
OG-03	**CRITICAL**	[CRITICAL] Every CRITICAL requirement shall map to at least one named regulatory clause. The mapping shall be approved by the Regulatory Affairs team.	21 CFR §11.10(a) ICH E6(R2) §5.5.1 SDPF Language Specification §11.3 Style 10

Regulatory Mapping Coverage Summary

Category	Count
CRITICAL requirements mapped (R-series)	7 (R-001 through R-005, R-009, R-010)
CRITICAL requirements mapped (OG-series)	3 (OG-01, OG-02, OG-03)
REQUIRED requirements mapped	3 (R-006, R-007, R-011)
OPTIONAL requirements mapped	1 (R-008)
Total requirements in specification	11 (R-001 through R-011) + 3 OG
Regulatory clause mappings	27
Frameworks covered	3 (21 CFR Part 11, 21 CFR §312, ICH E6(R2)) + HIPAA §164.312

S-12 Audit Evidence Requirements

Evidence Format

Field	Format	Description
specification_id	String	PHARMALOGIC-CTDMS-v1.0.0
style	String	10 — Compliance-Driven
stage	String	VERIFIED
problem_statement	Object	Full validated problem statement from S-00 P0-5
regulatory_frameworks	Array	[21 CFR Part 11, 21 CFR §312, ICH E6(R2)]
requirements_count	Integer	31
traceability_matrix	Object	REQ-ID to TEST-ID mapping per S-10
verification_timestamp	ISO 8601	UTC timestamp of verification gate execution
closure_status	String	COMPLETE
provenance_signature	String	HMAC-SHA256 signature

Retention Period

Minimum: 15 years from trial completion date per 21 CFR §312.62

Signing Requirements

Requirement	Specification
Algorithm	HMAC-SHA256 (RFC 2104, FIPS 198-1)
Key Source	Secure environment variable; key not embedded in evidence package
Key Name	PHARMALOGIC_PROV_KEY_2026
Key ID	PL_PROV_2026_Q1
Verification	Any party with verification procedure and key can verify

Evidence Level Conformance

Level	Requirements
Level 1	Specification exists, style declared
Level 2	All 11 structural invariant checks pass
Level 3	HMAC-SHA256 signed, all fields present, CLOSURE STATUS = COMPLETE

S-13 Compliance Verification Procedure

Inspection Readiness Checklist

Item	Evidence Field	Inspector Question
1	traceability_matrix (S-10)	Show me your audit trail for Subject Visit Record modifications
2	provenance_signature (S-12)	How do you validate that your electronic records are authentic?
3	SPEC_LOCKED + VCR (S-09)	What is your system validation documentation?
4	R-007 regulatory mapping (S-11)	How long do you retain audit records?
5	verifying_entity + provenance_signature	Show me the record of who approved this release

Regulatory Clause Coverage Matrix

REQ-ID	21 CFR Part 11	ICH E6(R2)	FDA 21 CFR 312
R-001	§11.10(e)	§5.5.3	—
R-002	§11.10(e), §11.10(k)	—	—
R-003	§11.200(a)	§5.5.2	—
R-004	—	§4.11	§312.32(c)
R-005	§11.10(a)	—	—
R-006	§11.10(d)	—	HIPAA §164.312
R-007	—	§8.1	§312.62

Post-Release Conformance Protocol

1. Every CTDMS release SHALL produce a Level 3 evidence package
2. Evidence package SHALL be archived in validated DMS
3. RA team SHALL review inspection readiness before Q4 2026 inspection

4. SPC monitoring SHALL track correction cycles per feature
5. Control limits: UCL = 0.8 cycles (rolling 5-feature average)

Appendix A: Requirements Index

REQ-ID	Priority	Title
R-001	CRITICAL	Audit Trail — CRUD Operations (with ALCOA+ field diff)
R-002	CRITICAL	Audit Record Immutability
R-003	CRITICAL	Multi-Factor Authentication and Session Control
R-004	CRITICAL	Adverse Event Reporting — 7-Day and 15-Day Windows (FDA ESG / E2B R2)
R-005	CRITICAL	Verification Closure Record
R-006	REQUIRED	Data Encryption and Key Management
R-007	REQUIRED	Audit Log Retention with Trial Completion Trigger
R-008	OPTIONAL	Audit Summary Report (PDF/A-3)
R-009	CRITICAL	Electronic Signature — 21 CFR §11.50 / §11.70
R-010	CRITICAL	Role-Based Access Control — 21 CFR §11.10(d)
R-011	REQUIRED	Backup and Disaster Recovery — 21 CFR §11.10(c)

END OF SPECIFICATION

PHARMALOGIC-CTDMS-v1.0.0

SPEC_LOCKED: 2026-04-02T14:30:00Z

Verifying Entity: SDPF Desktop Studio v1.0