1. AI Retraining Pipeline, IMDRF N90 & §515C PCCP Attestation — arrhythmia_cnn_v1

Work Order: QSA-AIML-2026-011 | Frozen Commit SHA: c5b6ff9 | Model: arrhythmia_cnn_v1.safetensors

Engagement Track: Standalone AI/SaMD MLOps, IMDRF N90 (Aug 2026) / FDA §515C PCCP & Non-Human Identity Sprint ($12.5K-$18.5K | 4 Days)

Pipeline Verdict: ZERO-PICKLE & HSM-SIGNED PCCP LOCKED (Compliant with 21 CFR 892.2055, IMDRF N90 Final & EU AI Act Art. 15)

Securing the Regulated MLOps Pipeline Against Adulteration

• The Pipeline Is the Regulated Device: Under FD&C Act §515C and IMDRF N90 (Aug 2026), unauthorized CI/CD weight swaps, leaked non-human API tokens, or out-of-spec retraining runs render shipped AI updates legally adulterated.

2. IMDRF N90 (Aug 2026), FDA §515C & Non-Human Identity MLOps Gate

1. FD&C Act §515C, 21 CFR 892.2055 & IMDRF/SaMD WG/N90 FINAL (Aug 2026) MLOps Audit

Evaluates the regulated MLOps retraining, weight-signing, and deployment pipeline across the three mandatory IMDRF N90 / FDA §515C PCCP pillars (*Description of Changes*, *Change Plan / Modification Protocol*, and *Impact Assessment*) plus EU AI Act (2024/1689) Art. 15 & Art. 43(4):

MLOps / PCCP Security Gate	Governing Standard (2026)	Verified Pipeline Control (arrhythmia_cnn_v1.safetensors)	Status
Zero-Deserialization Model Format	CWE-502 / MITRE ATLAS AML.T0010	Pure safetensors / bounded ONNX graph (0 Python pickle opcodes)	VERIFIED
Non-Human Identity (NHI) CI/CD Signing	OIDC Workload Identity + FIPS 140-3 HSM	Short-lived AWS/GitHub OIDC tokens (0 static long-lived CI secrets); offline HSM signs Ed25519 + ML-DSA-65 model weights	VERIFIED
Training Data Poisoning & Drift Lock	IMDRF N90 Change Plan / EU AI Act Art. 15	SHA-256 immutable training-cohort manifest + bounded sensitivity/specificity acceptance gate prior to promotion	LOCKED
Adulteration Guard & Atomic Rollback	FD&C Act §515C Deviation Rule / N90 Sec. 5	Automated CI gate blocks out-of-bound weights from shipping; signed MCUboot/container rollback to baseline c5b6ff9	FDA & HC READY