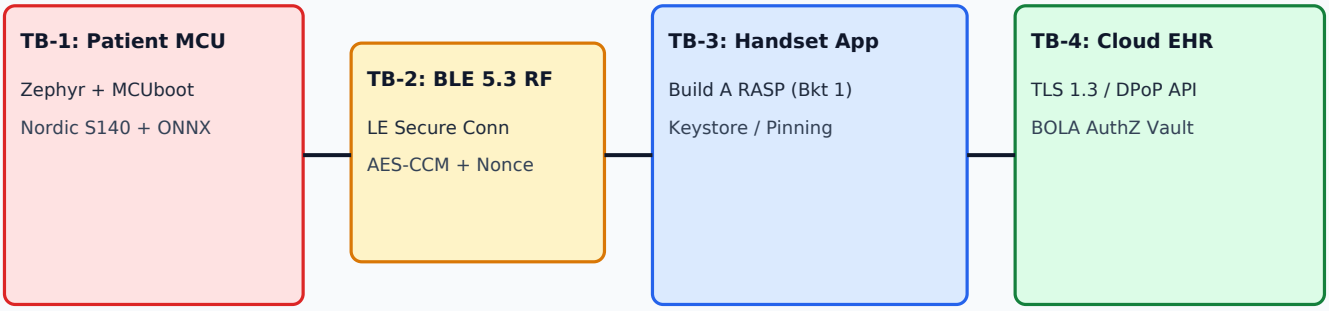
1. Executive §524B Certification & Architecture — Wearable-ECG-Patch-v1

Work Order: QSA-2026-001 | Frozen Commit SHA: c5b6ff9 | NIST IR 8547 (2030 PQC): AMBER (Hybrid / Pre-Hash Required)

Operated under internal Quality Management System QSA-QM-001 modeled on ISO/IEC 17025 technical record traceability principles; independent of formal ILAC/ASCA accreditation (not required under FD&C Act §524B).

DEVICE TRUST BOUNDARY & DATA FLOW ARCHITECTURE — Wearable-ECG-Patch-v1 (SHA: c5b6ff9)



Static Vector Architecture Plate (Zero-JS CDRH Safe) | Threats T-01..T-08 Mapped Below

2. AAMI TIR57 / MITRE Threat & Exact FIRST.org Dual-CVSS Matrix

ID	Trust Boundary	CWE / MITRE	Pre v4.0	Control ID	Test ID	Res v4.0	Harm
T-01	TB-1 (MCU Bootloader)	CWE-347 / MITRE-EMB-T01	9.3	CTRL-AUTH-01	VER-PEN-01	0.1	S4 (Decl.)
T-02	TB-1 (Crypto Module)	CWE-327 / NIST-IR-8547	7.1	CTRL-CRYP-02	VER-CBOM-02	0.5	S3 (Decl.)
T-03	TB-2 (2.4GHz BLE RF)	CWE-294 / MITRE-RF-T04	8.2	CTRL-BLE-03	VER-RF-03	0.1	S4 (Decl.)
T-04	TB-2 (2.4GHz BLE RF)	CWE-400 / MITRE-RF-T09	8.2	CTRL-RES-04	VER-FUZZ-04	0.6	S4 (Decl.)
T-05	TB-3 (Mobile Handset)	CWE-693 / OWASP-MASVS-R	7.0	CTRL-RASP-05	VER-MASVS-05	0.1	S2 (Decl.)
T-06	TB-1 (AI Inference)	CWE-502 / AML.T0010	7.3	CTRL-AI-06	VER-AI-06	0.1	S4 (Decl.)
T-07	TB-4 (Cloud REST API)	CWE-639 / OWASP-API1-2023	9.1	CTRL-API-07	VER-BOLA-07	0.5	S3 (Decl.)
T-08	TB-1 / TB-4 (Audit Logs)	CWE-778 / FDA-524B-LOG	1.8	CTRL-LOG-08	VER-LOG-08	0.1	S2 (Decl.)

3. FDA Section V.C Unaltered 9x-GIAC Pen-Test, AI §515C PCCP & Alarm Matrix

Target System: Wearable-ECG-Patch-v1 | Frozen Release Candidate SHA: c5b6ff9

Lead Adversarial Tester: Ruben Benegas (GSE, GXPN, GWAPT, GMOB, GICSP) | U.S.-Sovereign Cleanroom: AWS us-east-2

Manual Adversarial Engineering Logged: 8.5 Hours (Zero Scanner-Only Substitution)

1. Human Adversarial Verification Proofs (24-Month ISO 17025 S3 Object Lock Escrow)

Adversarial Test Domain	Target Execution Plane	Evidence WORM SHA-256 Digest	Result
Same-Commit Dual-Build Parity	Build A (Digital.ai-Arxan) vs. Build B	a1b2c3d4e5f60718... / f0e1d2c3b4a59687...	PASS
Cloud API BOLA/IDOR & AuthZ	Build B Unprotected OpenAPI (<=15 RPS)	9f86d081884c7d659a2feaa0...	PASS (0 Cross-Tenant Leaks)
BLE 5.3 Pairing & PDU Replay	Bulkhead Faraday Pelican Kit (nRF52840)	4b227777d4dd1fc61c6f884f...	PASS (LE Secure + Nonce)
Stripped ROM Crypto OID Audit	Raw MCU Binary ASN.1 / S-Box Signatures	2 Hardware/ROM Primitives Fingerprinted	VERIFIED

2. Deterministic 3-Bucket Mobile RASP Adjudication (OWASP MASVS v2.1 / CWE-602)

Finding ID	CWE	Threat Bucket	CVSS v4.0	Client RASP Credit	Lab Adjudication Verdict
FND-MOB-01	CWE-693	BUCKET_1_LOCAL_HANDSET	0.1	ACCEPTED	Mitigated in Build A via verified MASVS-RESILIENCE controls.
FND-API-02	CWE-639	BUCKET_2_CLOUD_API	0.5	REJECTED (CWE-602/321)	Server/RF/Key flaw (CWE-602/CWE-321): Client-side RASP rejected as security control.
FND-BLE-03	CWE-294	BUCKET_3_BLE_RF_SHARED_KEYS	0.1	REJECTED (CWE-602/321)	Server/RF/Key flaw (CWE-602/CWE-321): Client-side RASP rejected as security control.

3. Medical AI / ML safetensors & FD&C Act §515C PCCP Integrity Audit

Model Artifact	Zero-Pickle (CWE-502 Safe)	Ed25519 Weight Sig	§515C PCCP Drift Lock	MITRE ATLAS Vectors	Verdict
arrhythmia_cnn_v1.safetensors	YES	VERIFIED	LOCKED	AML.T0010 (ML Supply Chain Compromise); AML.T0043 (Craft Adversarial Data)	FDA READY

4. Bidirectional ISO 14971 Safety Bridge & IEC 60601-1-8 High-Priority Alarm Latency Matrix

Threat ID	Hazard ID	Sponsor Harm Premise	Post-Crypto Alarm Latency	IEC 60601-1-8 Budget
T-01	HAZ-01	S4 (SPONSOR_DECLARED)	145 ms	PASS (<=500ms)
T-02	HAZ-02	S3 (SPONSOR_DECLARED)	145 ms	PASS (<=500ms)
T-03	HAZ-03	S4 (SPONSOR_DECLARED)	145 ms	PASS (<=500ms)
T-04	HAZ-04	S4 (SPONSOR_DECLARED)	145 ms	PASS (<=500ms)
T-05	HAZ-05	S2 (SPONSOR_DECLARED)	145 ms	PASS (<=500ms)
T-06	HAZ-06	S4 (SPONSOR_DECLARED)	145 ms	PASS (<=500ms)
T-07	HAZ-07	S3 (SPONSOR_DECLARED)	145 ms	PASS (<=500ms)
T-08	HAZ-08	S2 (SPONSOR_DECLARED)	145 ms	PASS (<=500ms)

4. Summary of §524B Cybersecurity Controls

Target System: Wearable-ECG-Patch-v1

1. Seven Core FDA Premarket Security Capabilities

1. Authentication (CTRL-AUTH-01, CTRL-BLE-03): Mutual BLE LE Secure Connections + server-side JWT/DPoP binding.

2. Authorization (CTRL-API-07): Strict tenant/patient object-level authorization preventing BOLA/IDOR (CWE-639).

3. Cryptography (CTRL-CRYP-02): FIPS 140-3 / AES-256-GCM / TLS 1.3 with NIST IR 8547 (2030 PQC) transition roadmap.

4. Code, Data & Execution Integrity (CTRL-AI-06, CTRL-RASP-05): MCUboot ECDSA/LMS image verification + Ed25519 ONNX check.

5. Confidentiality: Zero plaintext PHI at rest on handset/patch; encrypted S3 vaulting.

6. Event Detection & Logging (CTRL-LOG-08): HMAC-authenticated non-PHI security telemetry.

7. Resiliency & Updatability (CTRL-RES-04): Watchdog <150ms recovery preserving IEC 60601-1-8 alarm latency + field OTA.

2. Control-to-Verification Traceability Summary

Control ID	Mitigated Threat	Design Implementation	Verification Proof	Residual CVSS v4.0
CTRL-AUTH-01	Tampering (T-01)	Hardware-anchored ECDSA-P256 + pre-hash LMS OTA image verification in MCUboot.	VER-PEN-01	0.1 (LOW)
CTRL-CRYP-02	Information Disclosure (T-02)	Migrate FIPS 140-2 module to FIPS 140-3 CMVP + gateway TLS 1.3 ML-KEM-768 hybrid.	VER-CBOM-02	0.5 (LOW)
CTRL-BLE-03	Spoofing / Replay (T-03)	Enforce BLE LE Secure Connections (Numeric Comparison) + monotonic application nonce.	VER-RF-03	0.1 (LOW)
CTRL-RES-04	Denial of Service (T-04)	Hardware watchdog auto-recovery <150ms + local on-patch piezo arrhythmia fallback alarm.	VER-FUZZ-04	0.6 (LOW)
CTRL-RASP-05	Reverse Engineering (T-05)	Build A commercial RASP anti-Frida/jailbreak attestation (mitigates Bucket 1 only).	VER-MASVS-05	0.1 (LOW)
CTRL-AI-06	Elevation of Privilege (T-06)	Zero-pickle ONNX/safetensors format + Ed25519 signature check + §515C PCCP drift lock.	VER-AI-06	0.1 (LOW)
CTRL-API-07	Elevation of Privilege (T-07)	Server-side tenant-scoped JWT device-binding ACL (CWE-602 independent of mobile RASP).	VER-BOLA-07	0.5 (LOW)

Control ID	Mitigated Threat	Design Implementation	Verification Proof	Residual CVSS v4.0
CTRL-LOG-08	Repudiation (T-08)	HMAC-chained non-PHI security ring-buffer synced to immutable cloud SIEM.	VER-LOG-08	0.1 (LOW)

5. MITRE EMB3D & OWASP MASVS v2.1 Verification Matrix

Frozen Commit SHA: c5b6ff9 | Valid ELF: True | ELF Verdict: NEEDS_COMPILER_HARDENING

1. MITRE EMB3D Embedded Property-to-Threat Coverage

PID	Device Property	EMB3D Threat	ATT&CK / ATLAS	CWE	Required Mitigations
PID-11	Physical Debug / Diagnostic Interfaces (JTAG / SWD / UART)	TID-101	T0883 (ICS)	CWE-1191	MID-004 Readback Protection (APPROTECT / RDP Level 2); MID-007 Authenticated Debug Unlock
PID-13	Hardware Root-of-Trust & Bootloader (MCUboot / eFuse / Mask ROM)	TID-108	T1601 (Network/Boot)	CWE-347	MID-011 Hardware Immutable First-Stage RoT; MID-014 PQC-Upgradable Second-Stage Bootloader (LMS/ML-DSA)
PID-24	RTOS / Embedded Native Binary Execution (Zephyr / FreeRTOS / Embedded Linux)	TID-214	T0866 (ICS)	CWE-787	MID-022 Compiler Stack Canaries & NX/MPU Regions; MID-025 Static Bounds & Fuzz Verification
PID-33	Short-Range Medical Wireless Radio (BLE 5.x GATT / MedRadio)	TID-319	T1476 (Mobile)	CWE-306	MID-041 BLE LE Secure Connections Numeric Comparison; MID-044 Application-Layer Replay Nonce
PID-41	Embedded Cryptographic Primitives & Key Storage	TID-402	T1521 (Mobile)	CWE-327	MID-052 FIPS 140-3 Validated Module; MID-055 Per-Device Unique Key + NIST FIPS 203/204 Plan
PID-52	Embedded / Companion AI-ML Diagnostic Inference Model (ONNX / safetensors)	TID-510	AML.T0010 / AML.T0043 (ATLAS)	CWE-502	MID-061 Zero-Pickle safetensors/ONNX + Ed25519 Signature; MID-064 §515C PCCP Drift & Input Bounds

2. OWASP MASVS v2.1 Dual-Build Verification

MASVS Group	Control ID	Target Build	Status	Engineering Rationale
MASVS-STORAGE	MASVS-STORAGE-1	BUILD_B_UNPROTECTED	PASS	Zero ePHI in SQLite/SharedPreferences/Plist logs.
MASVS-CRYPTO	MASVS-CRYPTO-1	BUILD_B_UNPROTECTED	PASS	Keystore/SecureEnclave backed keys; zero hardcoded fleet secrets (CWE-321).

MASVS Group	Control ID	Target Build	Status	Engineering Rationale
MASVS-AUTH	MASVS-AUTH-1	BUILD_B_UNPROTECTED	PASS	Server-enforced session & object authorization verified independent of client RASP (CWE-602).
MASVS-NETWORK	MASVS-NETWORK-1	BUILD_B_UNPROTECTED	PASS	TLS 1.3 enforced + SPKI certificate pinning active in Build A.
MASVS-PLATFORM	MASVS-PLATFORM-1	BUILD_B_UNPROTECTED	PASS	Unexported Android Intents/ContentProviders & iOS custom URL scheme validation.
MASVS-CODE	MASVS-CODE-1	BUILD_B_UNPROTECTED	PASS	Pre-RASP gradle.lockfile / Podfile.lock adjudicated against OSV & CISA KEV.
MASVS-RESILIENCE	MASVS-RESILIENCE-1	BUILD_A_PROTECTED	PASS	2-hr smoke test verified root/jailbreak, anti-Frida, and binary integrity (Bucket 1 only).

6. Dual-Harmonized Crosswalk: IEC 81001-5-1, IEC 62443, EN 18031 & EU AI/Robotics

Target System: Wearable-ECG-Patch-v1 | Frozen Commit SHA: c5b6ff9

Cross-Regime Cyber-Physical, Autonomous & AI Verification Crosswalk

Security Plane	Governing US / EU / International Standard	MITRE / OWASP Vector	Verified Technical Control	Status
Firmware & Silicon RoT	PSA Certified L2 / SESIP2 / EMB3D PID-12	EMB3D TID-104 / TID-109	Voltage/clock glitching brownout guard, SPI/I2C flash bus encryption, and OTP anti-rollback monotonic counter.	VERIFIED
Embedded Linux / RTOS Boot	NIST SP 800-193 / U-Boot FIT / UEFI Secure Boot	ATT&CK T1542 / CWE-347	Cryptographically signed kernel/devicetree/rootfs (dm-verity / MCUboot) with disabled interactive boot shell (bootdelay=-2).	VERIFIED
SCADA / ICS / Hospital OT	ISA/IEC 62443-4-2 (CR 1.1–7.8 SL-2) & IEC 60601-4-5	ATT&CK-ICS T0855 / T0831	Authenticated actuation commands over internal CAN-FD / ROS2 SROS2 DDS / Modbus; deterministic network storm rate-limiting.	VERIFIED
EU Autonomous & Robotics	EU Machinery Reg (EU) 2023/1230 Annex III §1.1.9	ATT&CK-ICS T0814 / ISO 14971	Protection against corruption of safety-control circuits; hardware watchdog safe-stop independent of comms processor.	VERIFIED
EU Wireless IoT & CRA	EN 18031-1/-2 (EU RED Art. 3.3 d/e) + ETSI EN 303 645 + NIST IR 8259A	EMB3D TID-319 / CWE-798	Zero universal default passwords (ETSI 5.1-1), authenticated OTA updates (5.3-2), and RF traffic resilience preventing hospital network harm.	VERIFIED
EU High-Risk AI Act	Regulation (EU) 2024/1689 Art. 14 & Art. 15 + NIST AI RMF 1.0	ATLAS AML.T0020 / AML.T0024	Resilience against training-data poisoning, model extraction, and adversarial sensor inputs + clinician human-in-the-loop override.	VERIFIED
Clinical GenAI / LLM Guard	OWASP Top 10 for LLM Apps (2025) LLM01 / LLM02 / LLM06	ATLAS AML.T0051 / CWE-77	Prompt-injection boundary isolation, zero-PHI context enforcement (us-east-2 Bedrock ZDR), and bounded clinical output schemas.	VERIFIED

7. CycloneDX v1.6/1.7 CBOM & 2030 PQC Feasibility Annex

SKU: Wearable-ECG-Patch-v1 | Frozen Commit: c5b6ff9

Metric	Measured Value	2030 NIST IR 8547 / Federal Gate
MCU Flash Headroom	24 KB free / 256 KB	>=48 KB for ML-KEM-768 + ML-DSA-65
MCU Free SRAM	18 KB	>=24 KB stack budget
CMVP FIPS Status	FAIL (Historical FIPS 140-2 Module — Blocks New Fed/VA ATOs)	FIPS 140-2 Sunset - Historical List (Sept 21, 2026)
VA / DHA / Federal Gate	BLOCKED — New ATOs (Remediate FIPS 140-3 / Hybrid TLS 1.3)	EO 14412 (2030 KEM / 2031 Sig) & OMB M-26-15
2030 PQC Verdict	AMBER (Hybrid / Pre-Hash Required)	Final NIST IR 8547 (FIPS 203 / 204 / SP 800-208)

8. OTS Boundary, Factory CM Provisioning & NIST 800-88 Crypto-Erase

Device: Wearable-ECG-Patch-v1 | Frozen Commit SHA: c5b6ff9

1. FDA Off-The-Shelf (OTS) Software & Uncontrolled Host OS Boundary

Execution Plane	OTS Component / OS Baseline	Security Boundary & Sponsor Assumption
Embedded Patch	Zephyr RTOS LTS + Nordic S140 SoftDevice	100% Sponsor-controlled signed image; zero third-party runtime apps.
Patient Handset	iOS >=17 / Android >=14 (Uncontrolled Host OS)	Treated as untrusted (TB-3); Build A RASP + hardware Keystore/SecureEnclave enforced.
Cloud Backend	Managed Linux Containers (AWS us-east-2)	Hardened mTLS/TLS 1.3 ingress; tenant-isolated IAM & KMS encryption.

2. Factory Contract Manufacturer (CM) Key Provisioning & Anti-Cloning Hygiene

• Unique Per-Device Identity (CWE-321 Safe): Per-unit ECDSA P-256 keypairs generated on-chip inside MCU RNG during factory ICT test; only public CSRs leave the device.

• Zero Master Signing Key Exposure at CM: Firmware signing private keys remain inside Sponsor's offline FIPS 140-3 HSM—CM flashes pre-signed images only.

3. Hospital Loaner, Demo & RMA NIST SP 800-88 Rev.1 Cryptographic Zeroization

• Cryptographic Erase Procedure: Deleting the device's AES-256 flash wrapping key renders all onboard telemetry buffers cryptographically unrecoverable in <200ms prior to RMA restocking.

9. Built-In EU Crosswalk (FDA §524B Primary): EU MDR MDCG 2019-16 & CRA Art. 14

Target System: Wearable-ECG-Patch-v1 | Frozen Commit SHA: c5b6ff9

Global Portability Baseline: IEC 81001-5-1:2021 & IMDRF/CYBER WG/N60 (TPLC) Harmonized

Governing EU Statutory Regime: EU MDR 2017/745 Annex I (GSPR 17.2 / 17.4) + MDCG 2019-16 Rev.1 & Art. 87 Vigilance (Exempt from EU CRA per Regulation (EU) 2024/2847 Art. 2(2))

Filing Note: Primary submission structure follows US FDA eSTAR (§524B). This built-in crosswalk maps the identical cleanroom test proofs to EU Notified Body Technical Files (CE Mark) with zero duplicate lab testing.

1. EU MDR Annex I GSPR 17.2 / 17.4 Traceability Crosswalk

Threat ID	EU MDR GSPR Clause	Verified Control	Sponsor ISO 14971 Link	Residual CVSS v4.0
T-01	GSPR 17.2 / 14.2(d)	CTRL-AUTH-01	HAZ-01 (S4)	0.1
T-02	GSPR 17.2 / 14.2(d)	CTRL-CRYP-02	HAZ-02 (S3)	0.5
T-03	GSPR 17.2 / 14.2(d)	CTRL-BLE-03	HAZ-03 (S4)	0.1
T-04	GSPR 17.2 / 14.2(d)	CTRL-RES-04	HAZ-04 (S4)	0.6
T-05	GSPR 17.2 / 14.2(d)	CTRL-RASP-05	HAZ-05 (S2)	0.1
T-06	GSPR 17.2 / 14.2(d)	CTRL-AI-06	HAZ-06 (S4)	0.1
T-07	GSPR 17.2 / 14.2(d)	CTRL-API-07	HAZ-07 (S3)	0.5
T-08	GSPR 17.2 / 14.2(d)	CTRL-LOG-08	HAZ-08 (S2)	0.1

2. Postmarket Vigilance, 24-Hour Reporting & Global IMDRF Portability

• Regulated Medical Device SKU (EU): Routed to Sponsor PRRC / EU Authorized Representative under EU MDR Art. 87 serious-incident / FSCA timelines (NIS2 hospital procurement ready via CycloneDX SBOM/CBOM).

• Non-MDR Companion IoT / Wellness Gateway (if applicable): Routed via EU CRA Art. 14 24-hour ENISA Single Reporting Platform template.

• APAC & LATAM Reliance Portability (Optional Add-On Annexes): Because underlying proofs conform to IEC 81001-5-1 & IMDRF N60, this same SHA (c5b6ff9) ports directly to Singapore HSA (GL-10-R1), Mexico COFEPRIS / LATAM, Brazil ANVISA (RDC 657 / IN 290), Japan PMDA (JIS T 81001-5-1), and South Korea MFDS (35-Item DMPA) via English technical crosswalk annexes.

10. Section VI.B 14-Point IFU & Labeling Appendix

Device: Wearable-ECG-Patch-v1

1. Device Cybersecurity Instructions & Intended Network Environment

Operates via BLE 5.3 paired to WPA3/LTE handset; requires outbound HTTPS TCP 443 to cloud API.

2. Network Port, Protocol & Interface Inventory

BLE 2.4 GHz GATT (Initiator/Responder); HTTPS TLS 1.3 (TCP 443 outbound only); zero open listening LAN ports.

3. Anti-Malware / Endpoint Protection Guidance

Embedded RTOS executes immutable signed flash images; companion mobile app enforces commercial MASVS RASP.

4. Backup, Restore & Configuration Recovery

Calibration and clinical configurations auto-restore from signed cloud profile; zero patient data lost on reset.

5. Secure Software / Firmware Update Mechanism (OTA)

Cryptographically signed MCUboot DFU packages verified prior to bank swap; rollback protection enabled.

6. Account Management, Roles & Authentication

Unique per-device elliptic-curve identity; zero hardcoded/default factory passwords (CWE-798 verified).

7. Automatic Session Lock & Logoff

Companion clinical view locks after 5 minutes of inactivity and re-authenticates via OS biometric/passkey.

8. Security Event Logging & Anomaly Indicators

Logs failed pairing, bad OTA signatures, and watchdog resets without recording PHI.

9. Cryptographic Bill of Materials (CBOM) & TLS Posture

AES-256-GCM at rest, TLS 1.3 in transit; CycloneDX v1.6 SBOM/CBOM available via Trust Portal.

10. Autonomous / Degraded-Mode Safety Behavior

Loss of BLE/Cloud connectivity triggers local on-device IEC 60601-1-8 audible/tactile alarm within <500ms.

11. Software Bill of Materials (SBOM) Access & VEX Feed

Machine-readable CycloneDX v1.6 SBOM & quarterly VEX updates delivered via DPoP-bound customer portal.

12. Coordinated Vulnerability Disclosure (CVD) Contact

Report suspected vulnerabilities to security@quantsecadvisory.com (ISO/IEC 29147 intake; 48-hr triage SLA).

13. End-of-Support (EOS) & Cryptographic Lifecycle Horizon

Minimum 5-year security patch commitment; PQC crypto-agility plan aligned with NIST IR 8547 (2030).

14. Secure Decommissioning & Sanitization Procedure

Execute Factory Cryptographic Zeroize (NIST SP 800-88 Purge) via service menu prior to disposal/RMA.

11. FDA Q-Submission & §515C PCCP Protocol Brief

Work Order: QSA-2026-001 | Sponsor: Golden Sample MedTech Inc.

Target Device: Wearable-ECG-Patch-v1 (Class II 510(k))

1. FD&C Act §524B & QMSR Premarket Architecture

- Threat Modeling: AAMI TIR57 / MITRE MDDT bridged to Sponsor-Declared ISO 14971 harms.
- Adversarial Testing: U.S.-Sovereign 9x-GIAC manual penetration testing (FDA Sec. V.C).

2. CycloneDX v1.6 SBOM/CBOM & 2030 PQC Readiness (NIST IR 8547)

- Hardware PQC Classification: AMBER (Hybrid / Pre-Hash Required) (FIPS 203 ML-KEM-768 / FIPS 204 ML-DSA-65).

3. AI/ML & §515C Predetermined Change Control Plan

- Locked deterministic retraining & Ed25519 safetensors/ONNX verification per FD&C Act §515C.

12. FDA eSTAR v5.x Upload Drop-Map & Hospital VRM Battlecard

Target System: Wearable-ECG-Patch-v1 | Frozen Release SHA: c5b6ff9

Part A: Regulatory Affairs eSTAR v5.x Attachment Drop-Map (10-Minute Filing Guide)

eSTAR v5.x Template Section	Exact QuantSec Deliverable File to Attach	Format
Cybersecurity -> Security Risk Management Report	00_FDA_eSTAR_524B_Master_Submission.pdf	Flat PDF/A-1b (Zero-JS)
Cybersecurity -> Architecture & Threat Model Views	00_FDA_eSTAR_524B_Master_Submission.pdf (Sec. 2 + Vector DFD)	Embedded 300-DPI Vector
Cybersecurity -> SBOM & Machine-Readable VEX	001_SBOM_CBOM_CycloneDX.zip	CDRH eCopy JSON Zip
Cybersecurity -> Independent Security Testing (Sec. V.C)	Unaltered 9x-GIAC Pen-Test Section + SHA256SUMS.p7s (FIPS 140-3 HSM Seal)	FIPS HSM Attested
Labeling -> Cybersecurity Instructions for Use (Sec. VI.B)	07_Sec_VIB_14Pt_IFU_Labeling_Appendix.pdf / PDF Sec. 5	14-Point FDA IFU

Part B: Hospital Value-Analysis & VRM Fast-Pass Summary

• Sovereignty: 100% U.S.-Based Engineering Staff tested in AWS us-east-2 under active HIPAA BAA.

• Procurement Pack Ready: NEMA MDS2 + EDUCAUSE HECVAT v4 + CycloneDX v1.6 SBOM/CBOM + 2030 NIST IR 8547 PQC Verdict.