1. HIPAA 91 FR 74848 (Nov 19, 2026) Patient API Security Attestation — Wearable-ECG-Patch-v1

Work Order: QSA-HIP-2026-012 | Frozen Commit SHA: c5b6ff9 | Federal Register: 91 FR 74848 (Published Nov 19, 2026)

Engagement Track: HIPAA 91 FR 74848 15-Day Patient/PHA Access API, BOLA & Zero-Tracker SDK Add-On (+$4,500 | 48 Hrs)

Statutory Gate: EFFECTIVE JAN 19, 2027 / MANDATORY COMPLIANCE JULY 19, 2027 (45 CFR 164.524 15-Day Access & Zero Ad-Tech PHI Leaks Verified)

Securing High-Speed 15-Day Patient & Personal Health App (PHA) API Exports

• Why 91 FR 74848 Requires Hardened API AuthZ: Cutting ePHI Right-of-Access turnaround in half (15 calendar days) while removing unreasonable patient verification friction requires bulletproof BOLA/IDOR (CWE-639) isolation, Passkey/DPoP token binding, and zero third-party tracking SDK leakage.

2. HHS HIPAA 91 FR 74848 (15-Day Access API & Zero-Tracker SDK) Matrix

1. HHS HIPAA Privacy Final Rule (91 FR 74848, Published Nov 19, 2026) Patient API & App Audit

Prepared ahead of the January 19, 2027 Effective Date and July 19, 2027 Mandatory Compliance Gate under 91 FR 74848 (45 CFR 160 / 164), which shortens individual ePHI Right-of-Access turnaround from 30 days to 15 calendar days and prohibits unreasonable identity-verification friction while maintaining strict ePHI API security:

91 FR 74848 / 45 CFR 164 Mandate	Clinical / Companion API Risk Vector	Verified QuantSec Control (Wearable-ECG-Patch-v1)	Verdict
45 CFR 164.524 (15-Calendar-Day Access)	High-velocity automated FHIR/REST patient & Personal Health App (PHA) exports triggering BOLA/IDOR (CWE-639)	Server-enforced patient-scoped JWT/OAuth2 + RFC 9449 DPoP sender-constrained tokens (VER-BOLA-07: 0 cross-patient leaks)	COMPLIANT
Frictionless Identity Verification (91 FR 74848)	Removing manual identity hurdles without opening credential-stuffing / ATO	Phishing-resistant OS Passkey / WebAuthn biometric binding (MASVS-AUTH-1)	COMPLIANT
Third-Party Tracking & Analytics Ban (OCR)	Impermissible ePHI leakage to ad-tech / crash-analytics SDKs in mobile apps	Static & dynamic Build B binary/network capture confirms zero Meta/Google/third-party tracking SDK ePHI exfiltration	ZERO TRACKERS
Care-Coordination Disclosures & BAA Transition	91 FR 74848 care-coordination APIs & July 19, 2027 BAA transition window	TLS 1.3 + AES-256-GCM payload encryption inside AWS us-east-2 HIPAA BAA enclave	BAA READY