Penetration Testing Scope for FDA Submissions: A 510(k) / De Novo / PMA Guide

How to scope a penetration test for an FDA submission. The full attack surface FDA reviewers expect (firmware, hardware, wireless, mobile, APIs, cloud), white-box vs black-box rationale, scope by pathway (510(k), De Novo, PMA, IDE), and the Letter of Attestation.

TL;DR

- Reviewers expect full-attack-surface coverage: firmware, hardware interfaces, wireless, mobile companion app, APIs, and cloud backend.
- White-box is the default - reviewers explicitly expect testers to leverage source code, threat models, and architecture documentation.
- A reviewer-ready engagement always produces a Letter of Attestation signed by the engagement lead.
- Scope depth differs by pathway: 510(k) maps to the predicate; De Novo and PMA require deeper architectural justification; IDE focuses on study-subject safety.

What "full attack surface" means

FDA's 2026 final premarket cybersecurity guidance expects the test report to demonstrate coverage of every interface a threat actor could reach. In practice, that means six distinct test domains:

- Firmware - secure boot, debug interfaces (JTAG/SWD/UART), update integrity, key storage, runtime integrity.
- Hardware - chip-level attack surface, side channels, fault injection where relevant to threat model.
- Wireless - BLE, Wi-Fi, cellular, NFC, proprietary RF. Pairing, encryption, GATT permissions, rogue-AP scenarios.
- Mobile companion app - iOS and Android: storage, transport, IPC, biometric handling, jailbreak/root checks.
- APIs - REST/GraphQL endpoints: authn, authz, IDOR, mass assignment, rate limiting, BAA-relevant logging.
- Cloud backend - tenancy isolation, IAM configuration, key management, logging integrity, data export paths.

White-box vs black-box: why white-box wins for FDA

The 2026 guidance says reviewers expect testers to leverage source code, threat models, and architecture documentation. That is white-box testing by definition. Black-box testing simulates an external attacker but consistently misses logic flaws in firmware update validation, key management, secure boot, and inter-component trust assumptions - exactly the controls that matter for patient safety. Default to white-box for premarket, reserve black-box for adversary-simulation scenarios after clearance.

Scope by submission pathway

510(k)

Full attack surface, white-box. Test plan should explicitly compare the cybersecurity attack surface to the predicate device, especially where you have added connectivity, mobile, or cloud beyond the predicate's footprint. Reviewers cite 'predicate divergence not addressed' often.

De Novo

Full attack surface, white-box, plus an architectural-justification section because there is no predicate. The pen test report should map findings against the security architecture you proposed in the De Novo classification request.

PMA

Deepest documentation requirement. Pen test evidence flows into the design history file with full traceability. PMA reviewers frequently coordinate with non-cyber reviewers (risk management, human factors) so the pen test report should be cross-referenced from the security risk assessment and the ISO 14971 risk file.

IDE

Scope focuses on whether unresolved cybersecurity risks could expose study subjects to unreasonable risk under 21 CFR §812.42. Pen testing must validate that compensating controls in the clinical environment are sufficient before enrollment.

The Letter of Attestation

A signed document from the testing firm stating that testing was conducted in accordance with the FDA premarket cybersecurity guidance, that the full attack surface was covered, and that every finding has been remediated or formally risk-accepted. Reviewers look for it because it confirms the test meets FDA-specific expectations rather than general IT-security best practice. Without one, expect a deficiency.

What a reviewer-ready report contains

1. Executive summary with risk-rated findings and Letter of Attestation reference. 2. Methodology section documenting white-box approach, tools, and standards (NIST SP 800-115, OWASP MASVS, OWASP ASVS, OWASP API Top 10). 3. Attack surface inventory with coverage notes per interface. 4. Findings written with severity (CVSS + clinical impact under ISO 14971), reproduction steps, evidence (screenshots, packet captures, code references), remediation, status. 5. Traceability appendix linking findings back to threat-model entries. 6. Signed Letter of Attestation.

Scope mistakes that get cited

- Mobile app tested but not in source-leveraged white-box mode (jailbreak detection bypassed in 30 minutes during reviewer follow-up).
- Cloud testing limited to OWASP API Top 10 scan - no tenancy or IAM validation.
- Wireless tested in protocol stack only, not at the radio layer.
- Firmware tested via released binary - secure boot and key storage not exercised.
- No Letter of Attestation - or a Letter that does not enumerate scope.

Frequently asked questions

Can the test be scoped to one attack surface, like firmware only?

Yes for postmarket validation or targeted risk work, but a scoped test will not satisfy the FDA premarket requirement for full-attack-surface coverage. Always mark scope explicitly in the Letter of Attestation so reviewers know what the report supports.

How long does a full-coverage engagement take?

Typically 3-5 weeks for a connected Class II device, 6-8 weeks for multi-device platforms with complex cloud and AI components. Week 1 is scoping and setup, weeks 2-3 are active testing, week 4 is remediation and retest, week 5 is final reporting.

What standards should the methodology cite?

NIST SP 800-115 for the overall approach, OWASP MASVS for mobile, OWASP ASVS and API Security Top 10 for web/API, OWASP IoT Top 10 for embedded, plus the FDA 2026 premarket guidance and ANSI/AAMI SW96. Listing the standards in the methodology section answers a question reviewers always ask.

Do you need our source code?

Yes for white-box, which is what FDA expects. Without source we can still execute the engagement but the report will be marked as black-box and reviewers will likely cite that as a deficiency.

How is medical device pen testing different from IT pen testing?

Three differences. Availability constraints (devices often cannot be taken offline mid-test), patient-safety mapping (every exploit evaluated under ISO 14971, not just CIA), and deliverable format (Letter of Attestation, threat-model traceability, FDA-formatted report).

Is retesting included?

For a reviewer-ready engagement it has to be. We retest every high and critical finding after remediation; the Letter of Attestation references the retest results. Vendors that charge separately for retest fragment the evidence chain reviewers expect to see.

Can a single report support FDA, EU MDR, and IEC 81001-5-1?

Yes if the methodology and evidence are structured for it. We include a process-evidence appendix that addresses notified-body questions on lifecycle integration so one engagement covers FDA premarket, EU MDR Annex I cybersecurity, and IEC 81001-5-1 verification.

Do you test in clinical environments?

Only when bench testing cannot reproduce a relevant condition (typically cloud and network-facing components). Clinical-environment testing uses non-disruptive techniques and tight operational windows coordinated with hospital ops.

What about AI/ML model components?

In scope when the device has any AI-DSF. Test plan extends to data-poisoning, evasion, model inversion, and prompt-injection scenarios using MITRE ATLAS and OWASP ML Top 10 as the framing. See our AI/ML Medical Device Security service.

What is the typical fixed-fee range?

Device-only (firmware + BLE) engagements typically land in the low five figures. Full-coverage engagements spanning firmware, hardware, wireless, mobile, APIs, and cloud typically run mid five figures. Multi-device or AI-heavy ecosystems run higher. The fixed fee includes Letter of Attestation, retesting of high/critical fixes, and FDA-formatted report - no add-ons.

Where to go next

- Medical Device Penetration Testing Service
- BLE & RF Penetration Testing
- Firmware Penetration Testing
- PHI Cloud Backend Penetration Testing

Ready to talk through your roadmap?

Book a Strategy Session →

Source guide: fda-penetration-testing-scope-510k. For the most current version, visit bluegoatcyber.com/guides/fda-penetration-testing-scope-510k.