Elexes

Medical Device Cybersecurity Standards Compliance Checklist (FDA + IEC)

FDA COMPLIANCE BASICS

- Is your device software-based or connected (wired, wireless, USB)?
- Have you followed the FDA's 2023 Premarket Cybersecurity Guidance and ensured compliance with requirements
- Have you prepared a cybersecurity plan, SBOM, and described your process of vulnerability disclosure, management and monitoring, cybersecurity incident management and threat modeling
- Have you assessed cybersecurity risks using tools such as threat modeling, penetration testing (can also be used for validation) etc

INTERNATIONAL STANDARDS ALIGNMENT

- Risk-based development lifecycle described (NIST-aligned)
- Have secure-by-design principles implemented and documented

SUBMISSION & DOCUMENTATION

- SBOM validated for completeness and accuracy
- Labeling reflects security controls and user actions
- A traceability matrix that maps cybersecurity risks to mitigations, test results, and residual risks

FINAL CHECKLIST BEFORE SUBMISSION

- Documentation is internally reviewed by a cybersecurity expert
- eSTAR/eCopy formatting (if applicable) confirmed
- Post-market plan for patching, ongoing threat monitoring, and vulnerability disclosure to be documented