Medical Device Cybersecurity

In today's connected world, medical technologies, from infusion pumps to AI-powered diagnostic tools, face escalating vulnerabilities due to their connectivity and integration with IT systems.

Cyber threats such as device hijacking or exploitation can impair device functionality or compromise patient data. In 2025, over half of connected medical devices were found to have critical vulnerabilities, and there has been a significant rise in unpatched devices nearing end-of-life.

To protect patients and preserve device integrity, medical device regulators demand rigorous compliance with country-specific guidance documents and international standards, such as **IEC 81001-5-1**, **ANSI/AAMI SW96**, and **AAMI TIR 57**.

Medical device manufacturers are challenged with implementing robust cybersecurity frameworks in addition to existing quality management systems, per FDA, EU MDR, and ISO 13485.

We will support you with cybersecurity compliance throughout the device life cycle, allowing you to build security into the device while we assist you with navigating complex cybersecurity requirements for medical device software. You will benefit from our extensive knowledge in medical device software regulatory requirements, resulting in a holistic implementation of cybersecurity requirements.

Our Services Include:

Cybersecurity Strategy & Advisory

- Regulatory gap analysis
- Security program development and roadmap
- Remediation strategy

Compliance Support

- Development of SOPs and templates
- IEC 81001-5-1, AAMI TIR 57 and ANSI/AAMI SW 96 implementation
- Cybersecurity DHF audit

Education & Training

- Custom workshops
- Introductory training

wega Informatik AG
St. Alban-Graben 3
4051 Basel

info@wega-it.com
+41 (61) 270 87 87

360° Services in Life Science, Pharma, and Healthcare Informatics