WRITTEN BY

AGNIESZKA STRZODA
Account Executive
Sii Poland

UNCOMPROMISED CYBERSECURITY

Bringing a medical device to the market is challenging, especially for companies with innovative ideas but limited resources and regulatory knowledge. The 2023 State of Cybersecurity for Medical Devices and Healthcare Systems report highlights a 59% increase in security vulnerabilities in healthcare software and firmware.

Sii provides a comprehensive suite of services to help companies navigate these challenges, focusing on cybersecurity, compliance, and quality assurance to ensure that medical devices meet the highest standards.

ENSURING QUALITY MANAGEMENT, RISK MITIGATION, AND SOFTWARE TESTING

Sii's holistic approach to medical device development addresses all key aspects, from quality management to cybersecurity.

A robust Quality Management System (QMS) ensures compliance and quality assurance in device development. Sii helps clients navigate QMS complexities, establishing continuous risk management frameworks to identify, evaluate, and mitigate risks from early development to market entry.

"Continuous risk management is essential for medical devices. Our frameworks help clients identify, assess, and mitigate risks effectively, ensuring safety and compliance," emphasizes Marcin Lis, Compliance and Medical Software Validation Specialist at Sii.

Thorough documentation is another critical compliance component. Delayed documentation can cause setbacks, and companies need to maintain detailed records throughout development, preventing last-minute issues.

Frequent changes in project scope can lead to increased costs and compromised quality. It is up to project management services to ensure these changes align with project goals and regulatory requirements, maintaining stability and focus.

Software testing is crucial for risk-critical devices. Specialized testing services should be provided, ensuring all requirements are met, and potential issues are addressed before market release.

COMPREHENSIVE CYBERSECURITY SOLUTIONS FOR MEDICAL DEVICES

Due to increasing digital interconnectivity, medical devices must be protected against cyber threats. Sii offers end-to-end cybersecurity support, covering threat modeling, security architecture, implementation, and continuous monitoring.

The Medical Device Security Suite includes:

- **Threat Modeling** – Identifying security requirements and ranking potential threats early.
- **Architecture & Design** – Tailoring a security architecture and countermeasures for identified threats.
- **Implementation** – Incorporating security best practices into application code.
- **Verification** – Conducting vulnerability assessments and penetration tests.
- **Monitoring** – Continuous vulnerability management for detecting security incidents.
- **Cybersecurity & ISO 14971** – Balancing security and safety controls without compromise.

"Cybersecurity is about more than protecting data—it safeguards patient trust and ensures the integrity of medical devices. Our comprehensive approach ensures security at every development stage," comments Dawid Jankowski, Cybersecurity Competency Center Director at Sii.

REGULATORY ASSURANCE SUITE

Meeting regulatory requirements is crucial for market entry and long-term success. Sii's Regulatory Assurance Suite streamlines this process, enabling clients to meet global standards efficiently.

"Navigating regulatory landscapes is one of the biggest challenges for medical device companies. Our suite streamlines compliance, ensuring all necessary standards are met efficiently," says Dawid Jankowski.

KEY AREAS COVERED BY THE REGULATORY ASSURANCE SUITE:

- **Identifying Regulatory Requirements** – Determining whether the product qualifies as a medical device.
- **Assessment** – Evaluating documentation and development processes against security requirements (e.g., MDR 2017/745, FDA 21 CFR Part 11).
- **Processes & Documentation** – Implementing QMS (ISO 13485), Risk Management (ISO 14971), and Software Development Life Cycle (IEC 62304).
- **Maintenance** – Managing documentation for market release and maintaining compliance.
- **Training** – Educating project teams to maintain high standards throughout the product lifecycle.

SUCCESS STORIES IN MEDICAL DEVICE SECURITY AND COMPLIANCE

Sii has successfully executed multiple projects addressing clients' compliance, cybersecurity, and quality assurance challenges.

EXPANDING US MARKET REACH FOR MOBILITY-ENHANCING DEVICES

A company specializing in mobility-enhancing products sought to enter the US market. Sii conducted a technical documentation review to ensure MDR and ISO 14971 compliance. The team updated software documentation in accordance with EN 62304, transitioned from MDD to MDR, prepared FDA application documentation, and oversaw conformity assessments in accordance with IEC 60601. This helped secure regulatory approval for the company's US expansion.

SECURING IOT DEVICES WITH ADVANCED PKI SOLUTIONS FOR QIAGEN

Qiagen, a global leader in molecular testing, introduced new IoT devices connected to a cloud-hosted application. They needed enhanced security for authentication and certificate management. Sii reviewed the initial PKI solution, designed an updated security architecture, documented necessary controls, and suggested future improvements. This ensured robust cybersecurity for Qiagen's IoT devices.

ENHANCING ULTRASOUND SCANNER PERFORMANCE

A leading medical device manufacturer partnered with Sii to improve the performance of 2D and 3D ultrasound scanners. Sii assembled a team of C++ engineers and testers to enhance system stability, optimize DICOM transmission, improve data transfer reliability, and extend system self-diagnostics. These upgrades ensured healthcare professionals could efficiently store, view, and share medical images across devices while maintaining stringent security and quality standards.

HELPING NAVIGATE THE COMPLEXITY

Developing medical devices requires technical expertise, compliance knowledge, and a dedication to quality and safety. Sii provides comprehensive support, including risk assessment, hardware and software development, thorough documentation, and certification assistance.