INSIGHTS
into **MedTech Innovation**

MEDACUITY

MEDICAL DEVICE DEVELOPMENT: DEMYSTIFYING THE PERCEIVED CONFLICT BETWEEN SECURITY AND INTEROPERABILITY

I recently participated in a MassDevice webinar titled, "Shaping HealthTech: Data Security, Modernization, and Beyond." The discussion delved into the intersection of the expanding interoperability of connected medical devices and the increasingly sophisticated cybersecurity threats they face. In this article, I further explore the convergence of security and interoperability and shed light on cybersecurity issues and lifecycle security concerns outlined in current FDA guidance.

– **Bruce Johnston, Lead Architect | MedAcuity**

Conflict? What Conflict?

A common theme I hear from people in the MedTech industry when talking about security is that there is a fundamental conflict between the interoperable exchange of data among connected devices and the need to secure those devices. Many assert that the protections required for modern security standards pose obstacles to connectivity, creating a burden for developers aiming to craft innovative systems that champion the inherent value of information sharing. However, the reality is that it is entirely possible to design and develop connected devices that harness the full potential of interoperability while prioritizing robust security measures. The key lies in integrating security as a fundamental component throughout the entire development lifecycle.

The Critical Role of Security in Connected MedTech Development

While an important consideration for all medical devices, security becomes increasingly crucial as medical technologies evolve to connect once standalone technologies into interconnected systems designed to facilitate the interoperable exchange of information. Innovation, patient safety, and system integrity concerns all converge in these complex systems. The seamless flow of data between devices within these interconnected systems is facilitating enhanced clinical decision-making and improved patient outcomes. Security plays a crucial role in this data flow because the data is only valuable if it can be trusted. Regulators have recognized this critical convergence and now require careful consideration of security throughout the design and development process for medical devices of all kinds.

Shortchanging the assessment of security during device development may seem like a way to accelerate timelines or reduce costs, but it often leads to avoidable setbacks and delays in realizing the vision of these interconnected systems. Consider the scenario where a failure to adequately examine security issues results in a Refuse to Accept (RTA) for the device submission. In our experience, even in the best-case scenario where the issue lies solely with the submission documentation, addressing the issues and resubmitting it could entail significant delays, often stretching to weeks. More often, however, an RTA is triggered by failure to perform critical assessments of security risks. Retroactively executing

those assessments can take weeks or months, further delaying the ultimate approval of the device. The mitigation of any issues found by the assessment—and issues are almost always found—will add further delays.

Mitigations may involve filling gaps in the QMS procedures and plans, adding requirements for new mitigations, analyzing impact of changes, updating designs, reviews, implementation, and re-verification. This degree of re-work all adds up, leading to months and months of delay for a program, creating time-to-market, budget, and schedule risks that ultimately affect the success of the program.

Security and the development of innovative, connected devices don't have to be conflicting forces. In fact, they can coexist harmoniously and achieving both is possible without a significant additional development effort. The key lies in elevating security to be a full participant and core requirement from the earliest phases of design and development. By incorporating security requirements as integral aspects of the product definition, akin to functional or performance requirements, the system is designed from the start to meet all essential security requirements.

Meeting the Challenges of Securing Connected Devices

Developing a holistic approach to integrate security into all the elements of modern medical technology development can raise a variety of challenges, including:

- The environment into which devices are deployed is constantly changing. The environment you see today will almost certainly not be the same environment in which a device will be operating in two, five, or 10 years from now. For manufacturers and developers of devices who want to "plug in" to an interconnected environment, the most important aspect of the software architecture and design is flexibility. The need to keep current with technological updates and software patches in medical systems is changing the traditional paradigm of monolithic releases with infrequent updates. Creating software architectures driven by attributes like extensibility, modifiability, and maintainability are essential to facilitate the adoption and efficient maintenance of devices across different environments.

- The interoperable exchange of data between devices in interconnected systems, such as delivery of data to an electronic health record (EHR) system, brings with it additional concerns about privacy and protection of patient data that necessitates the consideration of more than just FDA cybersecurity guidance. The flow of data in interconnected systems promises streamlined workflows, efficient communication, real-time monitoring, and improved care coordination. However, device designers must consider additional requirements for these systems based on regulations such as HIPAA and the GDPR. The goal is to ensure that the privacy and integrity of personal medical data remain protected from the device's inception to its decommissioning.

- Open-source software offers the potential to accelerate new product development but brings with it the risk of introducing unknown vulnerabilities and safety risks into the system. The key to using open-source, and other Software of Unknown Provenance (SOUP), is rigorous validation to ensure the software will perform as intended, combined with a robust post-market surveillance and maintenance plan to ensure it remains secure and effective over the lifetime of the device. Vigilance is essential to mitigate potential risks associated with the utilization of SOUP components within a device design.

- The diverse range of suppliers providing medical devices in an interconnected environment makes it a challenge to design devices that can consistently operate securely and connect seamlessly. Each healthcare facility has its unique mix of various components - network infrastructure, connected devices, EHR systems, etc. An important first step for manufacturers in dealing with this challenge is the adoption of standards in key areas. Standards like HL7, FHIR, and DICOM have been in place for years to facilitate data exchange and we've recently seen the establishment of security standards for medical devices, such as AAMI SW-96 and IEC 81001-5-1. Together these standards provide device manufacturers with a common roadmap for secure device development, ensuring compatibility and reliability in diverse healthcare settings.

While these challenges currently exist in the landscape of connected medical devices, this landscape is continually evolving with the introduction of new technologies, each bringing its own unique hurdles. Integrating AI and machine learning features into medical devices, for instance, will introduce new challenges. Securing both the models and the data used to train them becomes crucial to guarantee the continued safety, integrity, and effectiveness of AI-enabled devices.

Conclusion

The trajectory toward connected, interoperable devices is inherently linked to the implementation of robust security practices. While interconnected systems and the associated flow of data and information holds the promise of significant enhancements in healthcare outcomes, they also pose considerable risks and setbacks for device manufacturers. The perceived conflict between interoperability and security can become real when security considerations are deferred or neglected, and need to be applied to near complete designs. Failure to adopt a comprehensive security approach that ensures system integrity across its entire lifecycle can lead to unforeseen costs, delays, submission rejections, and recalls. Embracing a holistic strategy is not only essential for the success of connected MedTech devices but is paramount in mitigating potential challenges and maximizing their benefits.

ABOUT THE AUTHOR

Bruce Johnston | *Lead Architect*

Dr. Bruce Johnston has 25+ years' experience designing and developing complex software systems and 15+ years' experience working in regulated medical software development. Much of this experience has been focused on understanding and improving on the interaction of regulation and software development for Class II and Class III medical device programs. Most recently, Dr. Johnston has been providing strategic insight to a variety of clients on the implications of security in the development of interconnected software systems in the regulated medical environment.

Contact MedAcuity - info@medacuity.com

ABOUT MEDACUITY

MedAcuity, a software engineering firm, partners with companies to address the business and technical challenges inherent in developing complex software-intensive solutions. Offering a combination of strategic consulting services focused on aligning product technology strategy with business goals and full lifecycle software development expertise, we accelerate the pace of innovation for leading companies and innovators in the MedTech, Life Sciences and Robotics industries. With over a decade of experience in software design and development methodologies for highly regulated and compliance-driven environments, our technical capabilities span all levels of software from embedded systems to mobile devices, the cloud and enterprise technologies. Contact us at **medacuity.com**