INSIGHTS

into **MedTech Innovation**

MEDACUITY

MEDICAL DEVICES: CONNECTIVITY CONCERNS

The Connected Medical Device Transformation

The medical device industry is experiencing a generational transformation. Nearly every project we've done in the last several years is either connected or will be connected shortly.

Gone are the stand-alone devices of the past. From patients to providers (HCPs) to device OEMs to payers (including government), today all key players in the medical device value chain want to have the capability and flexibility that connected devices enable.

Common connected use cases include:

- Aggregation of data for patient safety (e.g., drug interaction detection)
- Clinical/diagnostic decision support systems
- Crowdsourced clinical inputs and outcomes
- Pay-as-you-go billing
- Consumables protection such as anti-counterfeiting
- Subscription services w/ automatic replenishment
- Maintenance and field service support features including predictive maintenance and real-time fault reporting
- Direct clinical interactions with telehealth/ telemedicine services `

> *"The global digital healthcare market is expanding, with a 16.13 percent annual growth rate expected through 2028; this growth is feeding demand for connected medical devices.[1]"*

Presently, the three main drivers through 2028 include the need for self-assessment, telehealth, teleconsultation, and telemedicine.[1] HCPs need support and workload reduction technologies due to this expansion. One approach is to make remote assessments easy and help healthcare professionals deliver the right consultation and medication, even for patients in remote areas.

Expansion of access to healthcare is a hot button topic in the news today, with digitization of care being a critical aspect. In this article, we'll dive deeper into the digital evolution that's well underway in MedTech. We'll also offer insights into how medical device OEMs can succeed in this complex landscape and ensure the acceptance of their premarket submissions, and ultimately, adoption of their products.

Complexity of Connected Medical Devices

While connected devices offer substantial potential benefits to various stakeholders, there are also **new risks** that need to be considered and potentially mitigated. Data breaches, network intrusion, and cybersecurity vulnerabilities in connected devices constantly call into question the reputation of an impacted organization. Failing to apply an appropriate level of expertise and diligence to understanding these risks can have substantial negative consequences, both financial and reputational.

Connected devices continue to rapidly evolve in the medical technology market. However, in contrast with other markets, such as the commercial and DoD sectors, networked systems have been developed and fielded for decades and have well-established precedent for connected devices, including cybersecurity concerns. Cyber threat modeling, attack surface reduction, IDS and IPS, and other security risk management practices in government and DoD are well matured and standardized (e.g., NIST SP 800-53, FIPS). These risk management and mitigation practices not only include software and physical devices, but also complex interconnected systems of systems. There is a wealth of knowledge and experience spanning many decades that the MedTech industry can draw on from the government, DoD, and commercial sectors.

> “ ***75% of more than 200,000 infusion pumps*** *on the networks of hospitals and other healthcare organizations had known security gaps.*[2] ”

Technical Considerations for Developing Next-Generation Connected Devices

Given the challenges in security risk management of interconnected systems, fully understanding the complexity of the solution you want to build is crucial. It is vital to consider all **regulatory guidance, industry best practices and the evolving threat landscape.** Furthermore, security hardening is not limited to the design phase of a project but extends to implementation and post-market operations as well. Technical implementation challenges (security, data privacy, device classification), UX and UI (use environments, users, etc.), and insider threats further complicate the situation.

In order to control security risk, whatever the source, it is crucial to apply **cohesive risk-based thinking** to address cross-cutting concerns and impacts often associated with security issues.

Some of the most important considerations we encounter are:

- Staying current with recent FDA guidance
- HHS (data privacy) and HIPPA compliance
- Attack vectors and vulnerability surveillance
- Geographic considerations around data rights and data governance
- Patient privacy

Investing in solutions for long-term compliance, maintenance, and operations, from really applying CI/CD and TDD, to test stands and test automation, and now mandated post-market surveillance carries big upfront costs but provide substantial ROI when applied thoughtfully.

The sandbox you once knew is gone when you transition from a stand-alone to a connected device. It’s crucial that device OEMs understand that the development cost, operational cost, and overall complexity goes well beyond the saleable features of the product. We want to make sure that they know how to evaluate the whole lifecycle ROI proposition before diving into R&D. The first step is always awareness.

The next step is to understand the moving parts and laying out the pieces of what now amounts to a **system of systems.** The device is just one part, the cloud infrastructure, the cloud applications, any connected peripherals, third-party integrations (EHR – FHIR, HL7, DICOM) must also be holistically considered. This is really development and understanding of the overall final architecture. There are many commercial reference architectures, but it is important to have the experience, understanding, and intuition to apply these to medical-specific concerns. That specialty involves understanding how to harmonize cutting-edge software industry practices with the application of ISO 14971, ISO 13485 and IEC 62304, and apply those practices to interconnected devices.

Additionally, all the associated FDA guidance documents, ranging from clinical to operational, must also be considered. We work with device OEMs through operational cyber risk assessments, post-market planning, and a whole host of operational IT concerns which were previously relegated to the CIO office. Many of these **operational concerns are now applicable to the engineering of your product.** The preparation of these materials is highly complex and requires specialized knowledge and experience. Even OEMs with strong traditional cyber experience frequently require assistance applying this new scope to their engineering practices and QMS.

Where Do You Start

This will sound somewhat basic, but from our experience, the **basis of all good software development** is to start with a **disciplined, regimented approach to solution architecture** guided by experience. It is especially important to start by applying sound engineering principles and experience-guided project planning. This is especially true of interconnected devices where the attack surface is the whole world, not just who's in the room. Invest in a strong product and software development foundation early in the process.

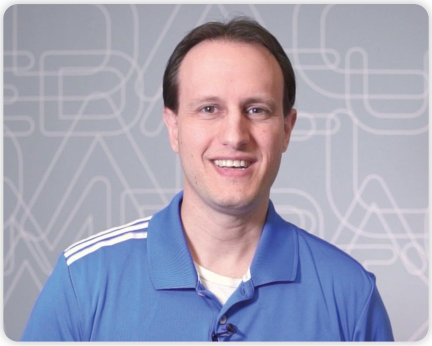
There is a big difference between engineering software for systems of systems and ad-hoc software practices in isolated devices. Ad-hoc software development approaches might be acceptable for certain applications but certainly not connected medical applications. We've seen many device OEMs suffer severe consequences from failing to **appreciate the scope, cost, and complexity** involved in bringing next-generation connected medical devices to market.

The FDA has greatly expanded their expectations for the careful consideration of not only safety risks, but also security risks associated with connected devices. Failing to meet these expectations can result in rejected submissions, recalls, and missed deadlines. The risk is just too high to the reputation of your company to get it wrong. Make the news for the right reason.

Our clients leverage our deep connected systems, distributed software, and regulatory experience to assess and improve everything relevant to connected device development. From tactical concerns to strategic organizational infrastructure considerations, our goal is to minimize their go-to-market risk. MedAcuity offers a wide range of services from up-front assessment and planning to regulatory-experienced full lifecycle software development, as well as gap analysis and remediation of acute problems.

ABOUT THE AUTHOR

Jeffrey "Jeff" Zampieron | *Solution Architect*



Jeff is a hands-on technical leader with domain expertise ranging from software, system, and security engineering to AI/ML-enabled systems. As a member of the Solution Architecture team at MedAcuity, Jeff applies his expertise to advise, consult, and support the development of complex connected medical devices for clients in the MedTech, Life Sciences, and Robotics industries. Jeff contributes to a few open-source projects and has given a number of interviews and talks in his areas of interest. He is an author of multiple patents and conference papers. Jeff holds a BS/MS in Computer Engineering from RIT.

Contact MedAcuity - info@medacuitysoftware.com

REFERENCES

1. *Medical Product Outsourcing, "Double-Digit Growth Ahead for Connected Medical Devices Market," March 15, 2022.*
2. *Unit 42 Palo Alto Networks*

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 **medacuitysoftware.com**