Key Considerations for the IoMT: Field Service Medical Event Debrief

by Pravin Kumar and Rodney Holmes

This year’s Field Service Medical conference focus was largely around reducing costs, minimizing risks and increasing value by providing superior service to customers, healthcare providers and ultimately to patients. The discussions, both in conference sessions and during networking, focused on how to harness digital trends around IoT, augmented reality and advanced analytics, all with an underlying thread of security and data privacy.

As with any transformational initiative, the move to the IoMT has huge benefits, but many potential challenges along the way. Here are just a few key things to consider as you pursue your IoMT journey.

1. **Technology and Interoperability** – While evaluating the IoMT landscape, consider open platforms following industry compliant protocols and data exchange formats. Connectivity and network bandwidth issues are primary infrastructure needs that should be assessed based on the specific use case being considered. Bridging outdated infrastructure and legacy devices with newer technologies and platforms will be an ongoing challenge. Consider retrofitting or upgrading existing devices with newer capabilities or replacing legacy devices with newer product models and phasing them out. The answer will vary based on the intent of use of the device, how the newer technology complements what is already in the field, and a deep understanding of the regulatory impact.

2. **Data Privacy** – The key question to ask is, “Who owns the data?” Is it the device manufacturer, the hospital, or the patient? Understanding how data will be used and consumed by different entities will determine the level of privacy to put in place to protect it. Clear risk-based data privacy policies must be defined, and regular audits performed, to ensure the data is safeguarded.

3. **Security** – Cybersecurity is a huge concern as devices move outside of hospital walls and become consumer-managed. These devices and their users are frequently connected via the various networks they encounter (coffee shops, libraries, home, office, etc.) which creates increased security risks. For hospitals, bringing devices into an existing network poses a big challenge. The solution is a security-focused assessment to analyze and rationalize the device onboarding process to accommodate a safe transition for devices. For data protection, it’s best to have a data-centric security model where access rules are built around data. This model should always be auditable and traceable to ensure data monitoring and tracking. As the IoMT device landscape continues to grow, every endpoint (or device) must be protected from potential cybersecurity risks to protect the interests of manufacturers and patients. This requires integrating automation and analytics, making it easier for both end users and IT professionals to stay on top of any data breaches. (Read this article on Nine Strategies to Secure the IoMT)

4. **Talent** – The IoMT transformation requires people with special skills to build, design, analyze and maintain IoMT applications. Without the right technical support, interoperability issues will never be overcome, and the risk of cyber security issues will become widespread. Organizations must educate current staff to prepare for future needs. They must also collaborate with academia and strategic partners while developing innovative recruiting and retention strategies to address any near-term shortages.

5. **Business Awareness and Readiness** – The IoMT will introduce new business models, and some of them will introduce significant change. With an increased focus towards outcome-based offerings, companies must build a strong collaboration between medical care providers, medical care payors and medtech companies to develop newer revenue models to improve patient outcomes and reduce health care costs. These collaborations should set clear expectations around the points at which they occur, as well as their governance and accountability structures. (Read this article on Building Support for an IoMT Program)

The potential benefits from the IoMT are enormous. At the heart of this transformation is the desire to improve patient care. As we heard at FSM, companies that invest time and effort to develop an IoMT strategy, explore new business models, reimage customer experiences, and build internal skills will ultimately lead the way. Are you ready?

**Learn More**

- **How to Build Internal Support for an IoMT Program**
  Here’s our advice for building a business case for IoMT initiatives, based on our experiences at the top medical device manufacturers in the world.

- **Securing the IoMT – Nine Strategies You Can’t Afford to Overlook**
  Protecting devices in the field requires an innovative approach to comprehensive information security. Here are nine security strategies to help mitigate risks while building a culture that enables innovation, compliance and operational effectiveness.
About the Authors

Pravin Kumar
pravin.kumar@kalypso.com

Rodney Holmes
rodney.holmes@kalypso.com
Rodney is Kalypso’s resident expert in remote service and management solutions for the MedTech industry.