Securing the IoMT – Nine Strategies You Can't Afford to Overlook

by Bryan Kissel and Chad Markle

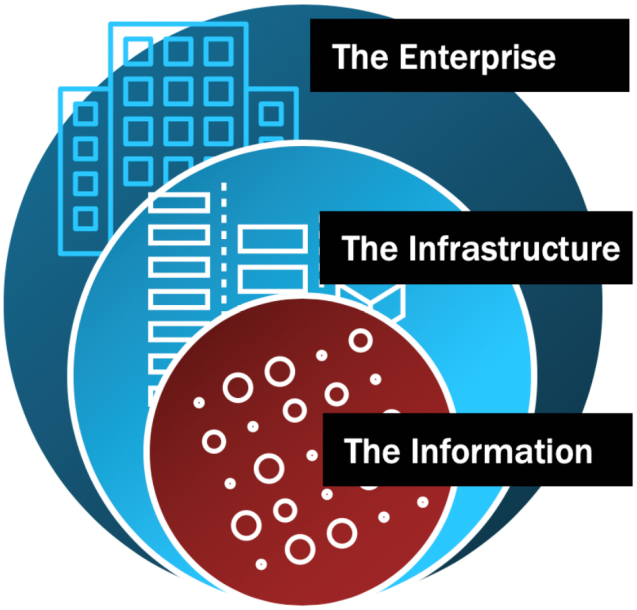
The headlines are full of stories about companies that fail to live up to the expectations and legal obligations of information security. Compliance is complicated, and it changes a lot.

For medical device companies with an Internet of Medical Things (IoMT) strategy, it's even more complex. Combine recommendations and frameworks like ISO 27001 and the PCI DSS with regulations like HIPPA, GDPR and MDR, and the magnitude of the challenge becomes very clear.

Companies are tasked with protecting both the connected devices in the field and the data they generate and transmit. So today's compliance strategies must include risk-based security practices protecting sensitive data and communications-based compliance practices around reporting, recording and archiving sensitive data.

Protecting devices in the field requires an innovative approach to comprehensive information security, along with compliance practices that can evolve alongside changing formfactors, design principles, connectivity solutions and management strategies. And on top of all this, interoperability and legacy device support is an ongoing, pressing need.

Nine Strategies to Secure the IoMT



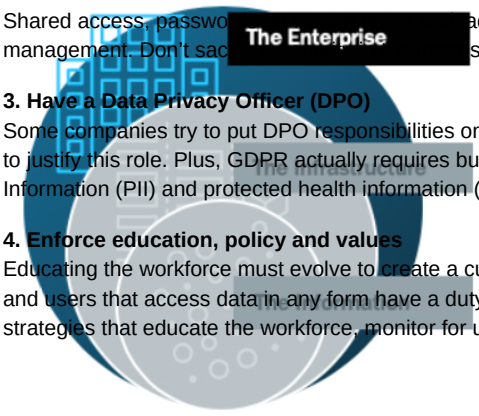
When physical security experts secure a house, they think in terms of concentric circles. The tree line or fence would your outer-most ring - whatever constitutes the perimeter. Next would be the front door and anything on the inner-perimeter, like cameras, a storm door or window locks. The inner-most ring would then be a panic room or secure space within the home. Each ring poses a more significant barrier than the last until you ultimately have your human assets within the inner-most ring protected by the increasing degrees of scrutiny as you move inward.

IT and Security professionals should approach security in much the same way. As you move closer to the center of the concentric rings, security controls should become increasingly strict, impeding risk vector access within each ring.

Securing the Outer Ring (The Enterprise)

In the outer-most ring is the true first line of defense – the policies and education practices of the enterprise. Enforcing strong, secure policies should be a part of any company's DNA, but here are a few strategies that must apply to this ring.

1. Use 'exceptionally' strong passwords
Eight-character passwords and mnemonic devices have led to many breaches, and most incidents are still user-related. Phishing, weak credentials and lost devices… we can do better.



Shared access, passwo admin/password' accounts represent the old ghosts of information security risk management. Don't sac st of deadlines or ease of use.

3. Have a Data Privacy Officer (DPO)
Some companies try to put DPO responsibilities on the CISO or a System Admin, but there's enough strategy, policy and education required to justify this role. Plus, GDPR actually requires businesses to have a named DPO responsible for managing Personally Identifiable Information (PII) and protected health information (PHI).

4. Enforce education, policy and values
Educating the workforce must evolve to create a culture of compliance at every level of operation. A clean desk policy is no longer enough, and users that access data in any form have a duty to protect that data and use it appropriately. The enterprise (led by the DPO) must deploy strategies that educate the workforce, monitor for user compliance and report incidents in real-time.

Securing the Inner Ring (The Infrastructure)

The inner ring represents the infrastructure – the hardware that supports applications and devices, secures pathways and manages traffic to assets. Innovation in this ring is critical to the longevity of connected medical devices and the operability of legacy devices still in use. There are many security strategies that apply specifically to this ring – here are some of the most important.

5. Innovate encryption strategies for micro-formfactor devices and implantables
Some of the most common medical devices, like implants and wearables, are the most vulnerable. Tiny Encryption Algorithms (TEA), system-derived passwords and [illegible] some options on the bleeding edge of device security, since many of these devices are too small to handle large encryption schemes.

6. Encrypt all the blind spots on the information superhighway
As more and more industries move toward cloud-based solutions and services, data managers must ensure that data is fully protected at every point in its lifecycle. Each system, node and relay must be demonstrably 'as-safe' as the last, from end to end.

7. Secure development of the entire IoMT ecosystem
A secure network or secure out-of-the-box solution is insufficient today. The complete ecosystems that support devices must be implemented with mature information security policies, governance, role-based access controls (RBAC) and deep documentation to ensure compliance across operational regions. Design with security in mind to always be 'audit-ready.'

Securing the Center Ring (The Information)

The center ring protects the most important asset at the heart of the IoMT – the data. Security at this level should be a nearly impenetrable shield of role-based access, attribute-based asset control, data type-specific archiving and retrieval, and comprehensive records retention.

8. Evolve and mature records management practices
Identifying and organizing data is the first and most important step to achieving compliance in any regulated industry. In the US, companies are tasked with securing data according to the risk associated with a breach. Considering the life or death implications of some connected medical devices and the truly personal nature of the data these devices generate, the medical device industry should expect the highest degree of scrutiny from auditors, legislators and even patients. New practices for records management – including documenting design, solution, architecture and audit materials – allow the DPO to demonstrate a reasonable and proactive approach to data security and privacy that lays the foundation for achieving compliance.

9. Manage the data like [illegible] it is
Insights gleaned from advanced analytics are the main ROI opportunity. To capitalize on this, data must be managed as a high-value asset. Protected health information and personally identifiable information should be considered as precious as secret business data, proprietary CAD elements, or IP.

In the age of Ransomware and PHI sales on the dark web, the question is no longer *when* a breach will occur, but *how much* an eventual breach will ultimately cost. As the IoMT evolves, isolated information security practices are a liability. Interoperability and security practices must extend to every point of the data lifecycle and be capable of growing alongside a maturing and ever-changing device landscape. As data privacy and information security continue to become almost inseparable, the offices of the CISO and DPO must evolve together, presenting a unified front against digital threats and a cooperative partnership in support of audit and compliance operations.

As medical device companies build and evolve an IoMT strategy, these efforts can help minimize risk while fostering a culture that mitigates information security risks, improving overall operational effectiveness, compliance posture and audit readiness.

Learn More

Kalypso's services for Life Sciences companies

Originally published on February 26th, 2019

What's your view? Add your question or comment

About the Authors

Bryan Kissel

bryan.kissel@kalypso.com

Bryan is a manager in Kalypso's digital practice. He is based out of Dallas and can usually be found programming synthesizers or cataloging compliance gaps to bring up again later.

Chad Markle

chad.markle@kalypso.com

Chad has over 25 years of experience working as an executive and advisor at Fortune 1000 companies to deliver results by combining strategic thinking with the transformative business impact of technology.