Product Security Maturity Assessment

Medical Device Security

Challenges our clients are facing

As technology continues to evolve and regulations and customers require more security, medical device manufacturers face new challenges to ensuring patient safety:

- Regulatory bodies are requiring higher standards of security for patient safety.
- International regulations have varying requirements that add complexity.
- Healthcare delivery organizations (HDOs) are expanding medical device security requirements.

Why act now?

Cybercriminals continue to target HDOs. To better enable patient safety, medical device manufacturers need to act now to enhance their products:

- Patients are becoming increasingly aware of safety concerns regarding the security of network-connected devices.
- HDOs have new security requirements that must be implemented into products to protect the safety of their patients.
- Negative publicity and headlines about cyberattacks on medical devices are leading to patient safety concerns.

Questions you should be asking

You should ask the following questions to reflect on the security of your medical device portfolio:

- Do we fully understand the security issues in our legacy devices?
- What security features do our customers care about?
- What security features are competitors adding that we should consider?
- Are we fully addressing new and emerging international regulations?
- Have we assessed the impact of new AI-enabled features?
- Does our medical device security operating model support our strategy?
- Does each product have a roadmap for improving security over time?

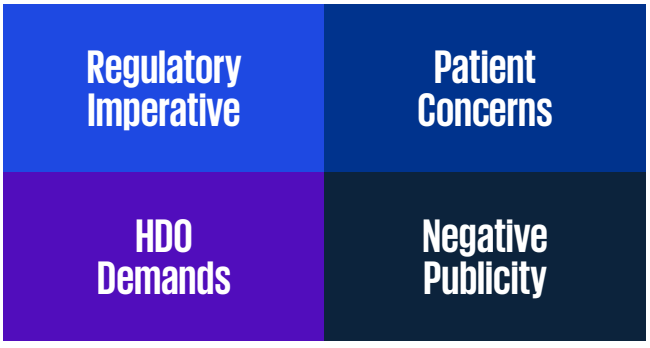

Image 1: Why act now?

What does KPMG deliver?

KPMG delivers a thorough strategic approach that evaluates the maturity of security pre/postmarket processes and product security features. This in-depth analysis provides valuable insights and enables businesses to optimize their security processes, manage their products effectively, and meet industry standards.

Our strategic approach

KPMG assesses the maturity of the program, divisions, and the products by leveraging a customized framework that aligns with industry standards, including the FDA pre/postmarket guidance, and the maturity of product security features:

- Process maturity provides insight into how well security by design is incorporated into the products and managed throughout the products' lifecycle.
- Product security features are crucial to understanding industry-expected and industry-exceeding security features across the product portfolio and are measured at the product level.

Key benefits:

- Gain a holistic view of both process and security feature maturity to fully understand your current state.
- Enable executive alignment and visibility to the medical device security program; drive awareness of the need for additional funding.
- Align the organization around a strategic improvement roadmap, including prioritized projects and clear milestones.

Ready to start?

Contact our team to discuss how KPMG can help on your medical device security journey.

Scott Erven
Principal,
Cyber Security Services
T: 719-332-6606
E: scotterven@kpmg.com

Adam Brand
Principal,
Cyber Security Services
T: 312-282-9878
E: adambrand@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**