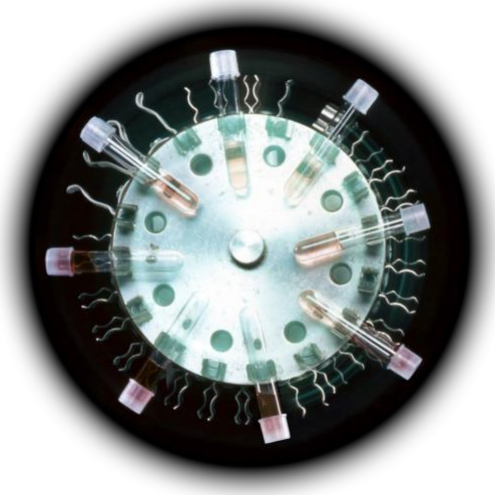
Deloitte.

Life Sciences and Health Care
Cyber and Regulatory Risk Services



Building and maintaining trustworthy and resilient medical devices

Medical Device Safety and Security (MeDSS)

Improving the customer experience and extending the connectivity of medical devices are top of mind for medical device manufacturers and health care delivery organizations. Medical devices provide many patient benefits as they become increasingly connected via the internet, networks, and other products or commercial systems. Cybersecurity and privacy concerns should be addressed in order to deploy this **technology everywhere** and provide **health care** to **anywhere**.

Medical device risks are evolving

The safety of medical devices has long been a concern of patients, health care delivery organizations, regulators, and the manufacturers of these devices. Traditionally, understanding the safety impacts of a medical device was based on clinical trials and safety risk assessments. As a result of innovation, medical devices began to include technology. This technology introduced a new risk area and an imperative consideration when determining the safety and trustworthiness of a medical device: cybersecurity.

Cybersecurity threats demand attention since they pose new risks to safety and privacy. A significant challenge associated with these medical devices is to balance their ability to improve and transform patient care with their associated risks.

International regulatory focus

Regulators such as the United States Food and Drug Administration (FDA), European Union (EU) Parliament, and China FDA issued regulations, guidance, and standards so that appropriate protections are built into medical device by design. In June 2013, the US FDA released a draft of its first medical device cybersecurity guidance titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices", which was published as final in June 2014 (FDA, 2014) . With this, the burden of proof of the safety of a medical device being submitted to the US FDA for premarket approval now had to include cybersecurity analysis and controls.

The environments in which connected medical devices operate are highly dynamic, marked by threats that change from one day to the next. Medical device manufacturers should not only embed cybersecurity, privacy, and safety premarket in product development, but also postmarket through ongoing and proactive threat and vulnerability monitoring and risk management in coordination with health care delivery organizations.

We can help—across the health care ecosystem

Deloitte's MeDSS services can help entities in the health care ecosystem—medical device manufacturers, health care delivery organizations, third-party and software providers, and digital health companies—potentially achieve better patient outcomes by lowering risks associated with advanced medical technology. Using a practical, business-centric approach we:

- Identify and help remediate cybersecurity and privacy gaps across the device lifecycle through security and privacy-by-design implementation
- Conduct vigilant post-market surveillance
- Help establish a resilient supporting infrastructure

The MeDSS team helps clients improve medical device cybersecurity and privacy practices as well as helps them strengthen the surrounding aspects of their broader information security and privacy programs and information technology capabilities. We advise many of the world's largest, technologically advanced global medical device manufacturers and health care delivery organizations on cybersecurity and privacy issues related to their connected medical devices through a wide range of services, including but not limited to:

- **Product Security and Privacy Program™ design, development, implementation, and operation:** Design, develop (policy, standards, procedures, work instructions, and templates), implement (including integration into the Quality Management System), and operate an enterprise-level Product Security and Privacy Program, which is designed to programmatically assist with securing connected products throughout their lifecycle.
- **Product security and privacy program maturity assessment:** Assess the maturity of the organization's product security and privacy program through documentation review and interviews; and develop a report to provide current state strengths, areas for improvement, recommendations, and a benchmark against the industry and peers.
- **Product security risk assessment:** Conduct a documentation review and interview-based security analysis eared at identifying device security vulnerabilities and associated threats, understanding the level of risk associated with identified vulnerabilities and threats, crafting remediation plans to bring risk to an acceptable /controlled level, and establishing information to serve as integration into safety risk analysis.
- **Technical security testing:** Leveraging Deloitte's Cyber IoT Studio located in Rosslyn, VA, conduct application, network, firmware, and hardware/firmware security testing geared at identifying device security vulnerabilities and attack vectors; understanding the level of risk associated with identified vulnerabilities; and crafting remediation plans to bring risk to an acceptable / controlled level.
- **Secure development support:** Support device development through security-by-design services throughout the development lifecycle including defining security requirements, performing threat modeling and integrating the output with device hazard analysis, conducting architecture reviews and third party security assessments, performing code analysis and vulnerability scanning, and creating security documentation as required by the Quality Management System.
- **Regulatory submissions support:** Assist in the development of documentation packages to aide in the submission of product security documentation to regulators for premarket approvals and post-market inquiries.
- **Postmarket security risk management:** Conduct ongoing security event handling to support postmarket device security risk management (e.g., threat intelligence, vulnerability monitoring and management, incident response) in alignment with Association for the Advancement of Medical Instrumentation (AAMI) TIR97:2019.
- **Supportive technology and tooling:** Design, develop, and implement a centralized tool to enhance the product security and privacy program, including tooling for security risk management and associated processes (e.g., asset inventorying, vulnerability management with bill of materials monitoring, customer communications), known as Deloitte's Product Security Manager™ platform, or Security incident and event management (e.g., SIEM) technology.
- **Product security and privacy transformation labs—Spark Experience:** Provide tailored training for product security and privacy executives to provide insight into industry leading practices and develop skills required to lead the product security and privacy program.

Contact us

For more information, please contact our MeDSS practice leadership:

Russell L. Jones
Partner | Deloitte Risk and Financial Advisory
MeDSS Global Leader
Deloitte & Touche LLP
Email: rujones@deloitte.com

Veronica Lim
Principal | Deloitte Risk and Financial Advisory
MeDSS Global Leader
Deloitte & Touche LLP
Email: vlim@deloitte.com

Phil Englert
Specialist Leader | Deloitte Risk and Financial Advisory
MeDSS Global Clinical Solutions Leader Deloitte & Touche LLP Email: penglert@deloitte.com

Nick Sikorski
Manager | Deloitte Risk and Financial Advisory
MeDSS Global Strategy and Solutions Leader
Deloitte & Touche LLP
Email: nsikorski@deloitte.com

For further information, visit our website at www.deloitte.com

Ongoing, collective efforts are required to drive continuous improvement in medical device safety. The MeDSS team contributes the insights we garner through project engagements to support the ongoing development of standards and industry guidance. Our recent work with the Association for the Advancement of Medical Instrumentation (AAMI) on TIR57:2016 and TIR97:2019, is one example of our commitment to helping manufacturers, health care delivery organizations, and patients themselves realize the potential of connected medical devices.