AdvaMed
Advanced Medical Technology Association

**Michael C. McNeil, Philips**
**AdvaMed, the Advanced Medical Technology Association**
**Testimony**

**Energy & Commerce Committee, Subcommittee on Oversight and Investigations**
**"Cybersecurity in the Heath Care Sector: Strengthening Public-Private Partnerships."**

**Tuesday, April 4, 2017**

Thank you Chairman Murphy, Ranking Member DeGette, and members of the Committee for the opportunity to testify today. My name is Michael C. McNeil, and I am testifying on behalf of Philips and our trade association, AdvaMed. As the Global Product Security and Services Officer at Philips, a leading healthcare technology company, my responsibility is to oversee efforts to ensure that consistent repeatable cybersecurity processes are deployed throughout the development and maintenance of products. Philips is driving the convergence between professional health systems and personal consumer technologies to seamlessly and securely connect devices, data, systems and people across the entire health continuum, from the hospital to the home.

AdvaMed is the world's largest trade association representing medical technology manufacturers. AdvaMed member companies produce the medical devices, diagnostic products and health information systems that are transforming health care through earlier disease detection, less invasive procedures and more effective treatments. Collectively, we are committed to ensuring patient access to life-saving and life-enhancing devices and other advanced medical technologies.

Let me first say a few words about Philips' cybersecurity strategy. Our strategy includes not just staying on top of emerging software-based vulnerabilities and potential external threats while anticipating how they might affect Philips products, it also includes collaborating with regulatory agencies, industry partners, and health care providers to close security loopholes. This includes participating in the Health Care Industry Cyber Security Task Force, under the auspices of the Department of Health and Human Services.

Working with these organizations, we can understand how other industries have addressed cybersecurity threats, identified challenges to health care environments, and provide health care industry stakeholders guidance on preparing for, and responding to, cybersecurity threats. Moreover, we can help develop effective and uniform application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.

We also work with health system partners like Augusta University Health, as part of visionary public-private programs like the one created by Governor Nathan Deal in Georgia, to address the cyber security challenges facing the US healthcare system. We also actively participate in industry groups like AdvaMed.

## Overview of Medical Technology Sector and Cybersecurity

Let me now describe an overview of the medical technology sector and cybersecurity. AdvaMed and its member companies, are committed to a robust cybersecurity framework as part of the development and postmarket management of medical technologies. Medical device manufacturers address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data. Similarly, manufacturers implement proactive measures to manage medical device cybersecurity, including but not limited to routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

## Principles for Robust Medical Technology Cybersecurity

Working with my colleagues at AdvaMed, we have developed the following five foundational principles for the management of medical device cybersecurity:

1. *Medical device development and security risk management*

First, an effective cybersecurity risk management program should incorporate both premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to disposal. In addition, medical device security risks should be addressed through a risk management process that is based on consensus-driven recognized standards and reference documents. This risk management process should include a process to monitor the ongoing security of devices in use.

2. *System-Level Security*

Second, medical technology cybersecurity is a shared responsibility among all stakeholders within the healthcare community. Because systems are only as secure as their weakest point, all elements of the system must be appropriately managed and secured.

3. *Coordinated Disclosure*

Third, medical device manufacturers should deploy a coordinated disclosure process that provides a pathway for researchers and others to submit information, including potential vulnerabilities, to the organization. Coordinated disclosure processes should clearly define the responsibilities of both the manufacturer and researcher. It is important to emphasize that whenever potential vulnerabilities involving a medical device are discovered, these findings should first be brought to the attention of the manufacturer and / or FDA for review, analysis, and possible remediation. Any other approach potentially places patients' lives at risk.

4. *Information Sharing*

Fourth, to assist manufacturers in continuously managing their device's cybersecurity throughout the product's lifecycle, industry should judiciously share threat and vulnerability information.

5. *Consensus Standards, Regulatory Requirements, and Education*

Finally, the development of cybersecurity-related consensus standards and regulations should be accomplished collaboratively among regulators, medical device manufacturers, independent security experts, academia, and health care delivery organizations. We also believe the health care industry should leverage the experiences and expertise of other critical infrastructure sectors and government agencies, such as NIST.

**Engagement with FDA and Public-Private Partnerships**

I would also like to take this opportunity to commend the U.S. Food and Drug Administration ("FDA" or "Agency") for its proactive leadership role over medical device cybersecurity. The FDA has worked closely with the medical technology industry and the broader healthcare ecosystem to ensure medical device cybersecurity is considered and addressed throughout all stages of product design and use. For example, in 2013, FDA released final guidance concerning premarket cybersecurity-related issues device manufacturers must consider when designing a connected medical device. And most recently, in December 2016, FDA released final guidance addressing the postmarket management of medical device cybersecurity. Taken together, these documents represent significant – and welcomed – achievements by the Agency to inform manufacturers of their medical device cybersecurity obligations.

Moreover, the FDA entered into a Memorandum of Understanding ("MOU") with the National Health Information Sharing and Analysis Organization ("NH-ISAC") and the Medical Device Innovation, Safety and Security Consortium ("MDISS") to promote cybersecurity information sharing for medical devices. These efforts have led to the creation of a medical device-specific information sharing and analysis organization, which has recently launched a program called the Medical Device Vulnerability Intelligence Program for Evaluation and Response, or MD-VIPER. MD-VIPER provides a streamlined mechanism for medical device manufacturers to submit and share information concerning cybersecurity-related issues, as well as other members of the broader healthcare ecosystem.

In light of the FDA's significant work and achievements to date, and the Agency's staff ongoing engagement with industry, we believe that the FDA serves as an example to all regulatory bodies with respect to the type of interaction, collaboration, and guidance an agency should provide to its regulated industry.

**Conclusion**

I want to underscore how critical it is to our industry that medical devices are safe for patients and risks, including cybersecurity threats, are appropriately and safely managed. Healthcare technology companies, like Philips, take seriously the need to continuously assess the security of their devices in a world where the risks, no matter how remote, evolve. Manufacturers make every effort to address cybersecurity throughout the product lifecycle, including during the design, development, production, distribution, deployment, maintenance and disposal of the device and associated data. Similarly, manufacturers implement proactive measures to manage medical device cybersecurity, including but not limited to routine device cyber maintenance, assessing postmarket information, employing risk-based approaches to characterizing vulnerabilities, and timely implementation of necessary actions.

We work very closely with the FDA and look forward to continuing to work with Congress and the Administration to ensure that the medical technology industry maintains a collaborative approach to cybersecurity and device safety.