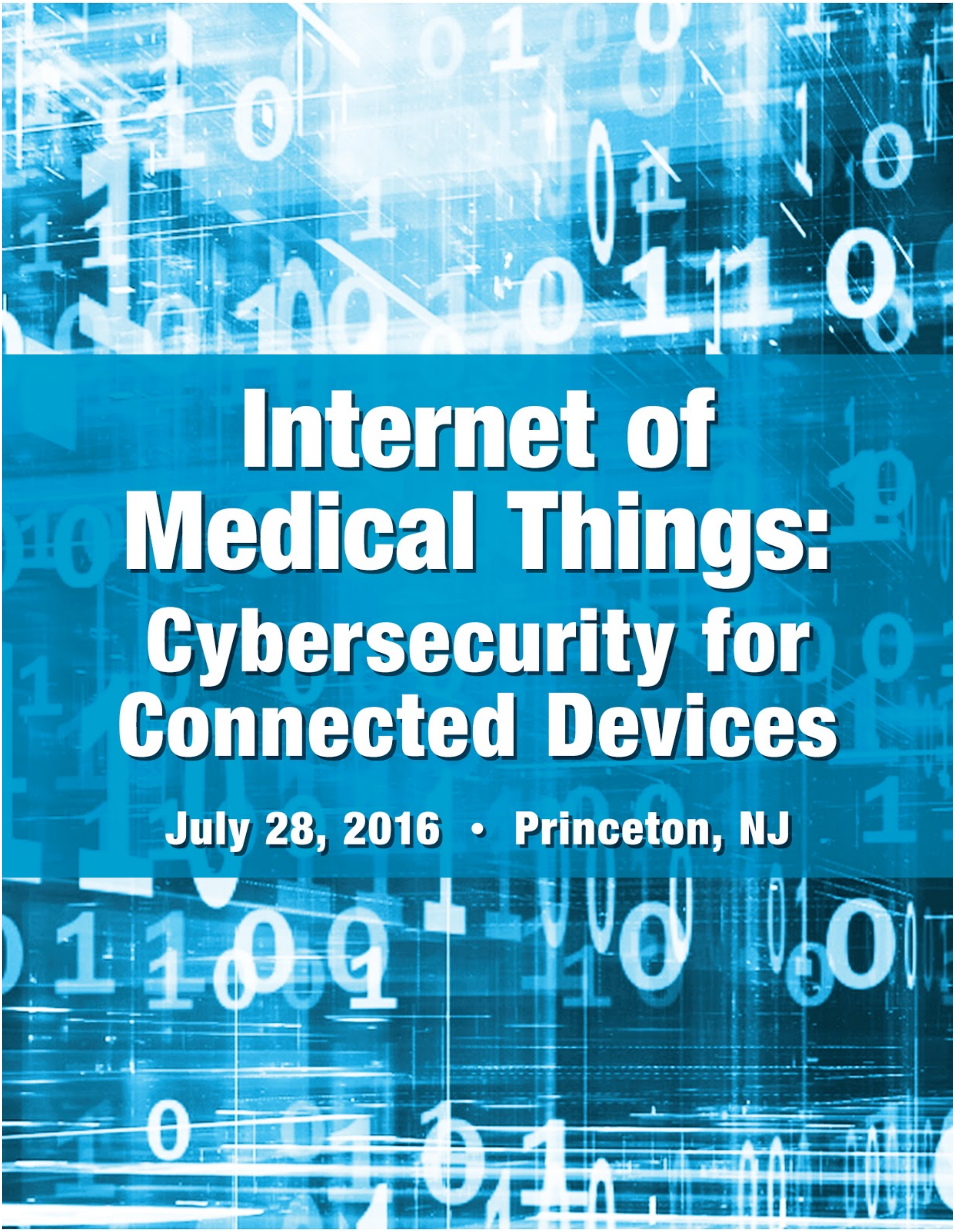

Internet of Medical Things: Cybersecurity for Connected Devices

July 28, 2016 • Princeton, NJ

Welcome to the Internet of Medical Things: Cybersecurity for Connected Devices.

Initiated in 2014 as the FDA was beginning to provide guidance that continues to evolve, this annual program addresses the quickly changing landscape that impacts patients, physicians, hospitals, engineers, IT departments, and researchers. The growth of implants, wearables, and robotics is opening vast opportunities for leveraging cloud computing, big data, and onboard analytics that can enhance and save lives.

Today we'll dig into the risks implied by this almost universal access, the agencies that are grappling with developing standards, and hospitals that need assurance that the very same innovations that provide so much benefit will comport with the security and privacy that their constituents expect.

In putting together our groundbreaking agenda, I particularly wish to thank our co-chairs, Colin Morgan and Rebecca Herold, as well as the full committee and our partner staff, listed below.

Finally, we could not have made today possible without the support and counsel of the many institutions and companies represented today. We welcome your feedback, and hope you will consider getting involved in planning IOMT for next year.

Best,

Joanne Gere
Executive Director
BioPharma Research Council

Thank You to our Co-Chairs	Colin Morgan, CISSP, GPEN Global Product Security, Sr. Manager Johnson & Johnson	Rebecca Herold CEO, The Privacy Professor Chief Visionary Officer / Co-Founder, SIMBUS360
Committee		
Miranda Alfonso-Williams Principal Consultant WAM Consulting Group	**Todd A Appleton** Former CIO Medical Devices	**Antonio Biancardi** Vice President DataForm Software
Dr. Robert Jamieson Chief Information Security & Privacy Officer Mallinckrodt Pharmaceuticals	**Sem Ponnambalam** President XAHIVE	**Judith Sheft** Associate Vice President Technology Development New Jersey Innovation Institute, NJIT
Jeanmarie Tenuto CEO Healthcare Technical Solutions	**Tom Fare, Ph.D.** Director, Strategic Alliances BioPharma Research Council	**Joanne Gere** Executive Director BioPharma Research Council

Thank You to our Partner Staff: BRC and PlanetConnect-

Richard Brandwein, Ronnye Schreiber, Gabrielle Flora, Susan Mehalick, John Onorato, Yulia Dorzhyeva, Sheritta Sessions, Melanie Walton, Jamesh Vindua

Save the Date!

Internet of Medical Things III: Cybersecurity for Connected Devices

Save the Date: July 27, 2017 • Princeton, NJ

Coming Soon:

Join us throughout the year- we welcome you to get involved with our committees, boards, and roundtables. Send a note to jgere@biopharmaresearchcouncil.org and we'll get started!

Point of Care Diagnostics: Design, Development, & Adoption

August 10, 2016 • 10:00am - 5:00pm EDT • Virtual Symposium

Microbiome Update 2016

October 5, 2016 • Institute for Life Science Entrepreneurship

Triangle Biotech Research Symposium V

October 11, 2016 • North Carolina Biotechnology Center, Research Triangle Park

R·P·M EXPO 2016

Regional Pharmaceutical Manufacturing

COMPANION DIAGNOSTICS

November 2-3, 2016 • Edison, NJ

BRC

www.biopharmaresearchcouncil.org

Wifi: CCenter Guest No Password is Needed

For Your Tweeting Pleasure: @BRCForum

Agenda

Internet of Medical Things: Cybersecurity for Medical Devices

9:15	**Welcome**	**Joanne Gere** Executive Director, BioPharma Research Council
9:20	**Keynote:** **Medical Device Security in a Connected World**	**Kevin McDonald** Director, Clinical Information Security, Mayo Clinic
10:00	**Historical Perspective:** **Solving the Mode 1** **Cybersecurity Problem**	**Dr. Robert Jamieson, Ed.D.** Chief Information Security & Privacy Officer Mallinckrodt Pharmaceuticals
10:15	**Managing Risk Across** **Diverse Devices**	**Shelby Kobes** Health Security Architect / President Kobes Security, INC
10:35	**Break**	
10:50	**Standards and Regulations Supporting** **Medical Device Cybersecurity and Privacy** **Panel Discussion** **Moderator:** **Rebecca Herold** CEO, The Privacy Professor Co-Founder & President, SIMBUS360 **Introduced by:** **Antonio Biancardi**, VP, DataForm Software	**Seth D. Carmody, Ph.D.** Cybersecurity Project Manager FDA Center for Devices and Radiological Health Office of the Center Director Emergency Preparedness/Operations & Medical Countermeasures **Nicholas P. Heesters, Jr., JD** Health Information Privacy & Security Specialist HIPAA Compliance & Enforcement U.S. Dept. of Health and Human Services Office for Civil Rights **Gavin W. O'Brien** Computer Scientist, NIST **William Ash** Strategic Program Manager for the IEEE Standards Association **Michael Geraghty** Director, NJ Cybersecurity & Communications Integration Cell New Jersey Office of Homeland Security and Preparedness
12:10	**Lunch**	
1:10	**Engineering Keynote:** **Setting Expectations with Vendors**	**Mitchell Parker** Chief Information Security Officer Temple University Health System
1:45	**Engineering Case Study/Workshop:** **Security by Design**	**Dave Saunders** VP Product Management and Development Galen Surgical Robotics **Wade Trappe** Professor, Dept. of Electrical and Computer Engineering Associate Director, Wireless Information Network Laboratory (WINLAB) Rutgers, The State University of New Jersey
3:00	**Break**	
3:15	**Roundtable:** **The Road Ahead-** **Perspectives from Manufacturers** **Introduced by:** **Ronnye Schreiber, President, PlanetConnect**	**Colin Morgan, CISSP, GPEN** Global Product Security, Sr. Manager, Johnson & Johnson **Roberta Hansen** Director, Digital Product Cybersecurity, Abbott
4:15	**Final Comments/Adjourn**	

Abstracts and Speakers:

Kevin McDonald
Director,
Clinical Information Security
Office of Information Security
Mayo Clinic

Keynote: Medical Device Security in a Connected World

Kevin McDonald has more than 35 years of healthcare experience. He holds degrees in Nursing, Education and Information Systems. His career has included direct patient care, management, electronic medical record implementation, and information technology and security. At Mayo Clinic one of his primary responsibilities is the security of medical devices.

Historical Perspective: Solving the Mode 1 Cybersecurity Problem

Dr. Robert Jamieson, Ed.D.
Chief Information Security &
Privacy Officer
Mallinckrodt
Pharmaceuticals

We have already transitioned into an era of device to device communications (IOT) and are rapidly adding the number of things that participate in these new ecosystems. At the same time, we are adding tremendous capabilities to benefit mankind and enhance our lives. Unfortunately these new technologies also come with significant increased cybersecurity risks that need to be addressed so that the devices aren't used to harm people or the systems that they were designed to benefit. To address these risks we must first solve our current cybersecurity problems (our Mode 1 problem) so we can create the cybersecurity solutions that will enable these technologies (Mode 2).

At Mallinckrodt Pharmaceutics, Dr. Jamieson is responsible for leading a global effort to provide a secure information/digital environment for the company's clients and internal users. Prior to this he was the Information Security Director for UL, LLC. Before working within the private sector, Bob served 22 years in the US Marine Corps where his primary focus was on Information/Data Security. His final assignment within the Marines was as the Commanding Officer of the Marine Corps School for Electronics. Bob holds a Bachelor's of Business Information Systems from National University, a Masters of Business Administration from University of Redlands, and a Doctor of Education in Organizational Leadership from Argosy University. He is CISSP certified.

Managing Risk Across Diverse Devices

Shelby Kobes
Health Security Architect/President
Kobes Security, INC

Though security systems are more complex than ever, we are still seeing major systems being compromised. IT departments have developed very mature systems and processes that allow them to protect some data and secure networks, from a network systems development and engineering perspective. Even with these systems in place, there is a disconnect between clinical engineering and information technology that is causing vulnerabilities.

In this presentation Shelby will discuss findings and security issues associated with medical devices from his current research and large hospital medical device security projects he has completed.

Common challenges and improvements that can be made by both hospitals and manufactures that will help improve security, privacy and health of the patient. He will present a plan to help prioritize medical devices, demonstrate current over the market hacking devices and address their potentials to cause issues within the hospital setting.

Shelby Kobes has been a medical device health industries consultant for the past 13 years, experiencing a variety of roles across healthcare and technology organizations. He has deep technical and academic experience in the security testing and organizational architecture of securing a variety of medical and diagnostic devices. Shelby has been involved in many initiatives domestically including a range of IT HIPAA/HITRUST assessments and medical device program development architectures for healthcare organizations. He has worked on medical device projects with Unity Point Healthcare System, OPTUM, UHG, Welmed, South West Medical Associates, and PWC Healthcare IT Risk and Privacy. Shelby has a MS in Information Security from Iowa State University College of Engineering, MA in Leadership, and a BA in Education.

Thank You to PlanetConnect

PlanetConnect, founding sponsor of the BRC, has been producing confidential, proprietary conferences for pharmaceutical and biotech companies for more than 20 years.

As a contributor to our growing and diverse community, PlanetConnect shares significant relationships with thought leaders across the complex and inspired life science landscape.

www.planetconnect.com

Panel Discussion

Standards and Regulations Supporting Medical Device Cybersecurity and Privacy

Rebecca Herold
CEO, The Privacy Professor
Co-Founder & President, SIMBUS360

Introduced by:
Antonio Biancardi
VP, DataForm Software

What types of cybersecurity protections and privacy controls should engineers build into medical devices? During this insightful roundtable discussion session the HHS OCR will describe the types of controls they expect to see in medical devices collecting, transmitting and storing patient health information, along with the obligations of medical device vendors that qualify as business associates under HIPAA.

The FDA will discuss recommendations for medical device cybersecurity. The DHS will describe the importance of medical device security for protecting the critical infrastructure. NIST and IEEE will share the standards that medical device engineers can use to build in security and privacy controls.

Panelists will address ways that all government agencies and standards bodies can provide each other support for ensuring medical device security and privacy is appropriately addressed by device manufacturers.

Rebecca Herold is an information privacy, security and compliance consultant, author and instructor who has provided assistance, advice, services, tools and products to organizations in a wide range of industries. She is a widely recognized and respected information security, privacy and compliance expert.

With more than 25 years of systems engineering, information security, privacy and compliance experience, she is CEO of The Privacy Professor ® consultancy she established in 2004, and is co-founder of SIMBUS360 Information Security, Privacy & Compliance cloud services.

She has authored 17 books and hundreds of articles. Rebecca appears monthly on the KCWI23 Great Day television show to raise public awareness of current information security and privacy topics.

She has been leading the NIST SGIP Smart Grid Privacy Subgroup since 2009, and has been in the IEEE Par 1912 Privacy and Security Architecture for Consumer Wireless Devices Working Group since mid-2015. She has also been an Adjunct Professor for the Norwich University MSISA program since 2005. Rebecca holds the following certifications: CISSP, CISA, CISM, CIPT, CIPM, CIPP/US, FLMI

Seth Carmody, Ph.D.
Cybersecurity Project Manager,
FDA Center for Devices and
Radiological Health,
Office of the Center Director,
Emergency Preparedness/Operations
& Medical Countermeasures

Dr. Carmody is currently on detail as the Cybersecurity Project Manager in the Office of the Center Director, Emergency Preparedness/Operations and Medical Countermeasures. Seth also serves as a subject matter and policy expert with CDRH's Cybersecurity Working Group.

He joined the FDA's Center for Devices and Radiological Health in 2011 as a medical device reviewer in the Division of Chemistry and Toxicology Devices where his duties focused on premarket approval of diabetes-centric devices and software recalls.

Nicholas Heesters
JD, CIPP, Health Information Privacy
& Security Specialist,
HIPAA Compliance & Enforcement,
U.S. Department of Health and Human
Services,
Office for Civil Rights

Nicholas Heesters is a certified information privacy professional with over 25 years of experience supporting technology and information security efforts in many diverse industries including financial services, government, defense, education and healthcare.

He earned his Bachelor of Science in Computer Science from the University of Delaware, his Master of Engineering in Computer and Software Engineering from Widener University, and his Juris Doctor from the Widener University School of Law. Currently, Mr. Heesters works for the U.S. Department of Health and Human Services Office for Civil Rights supporting HIPAA compliance and enforcement activities.

Gavin W. O'Brien
Computer Scientist
NIST

Gavin O'Brien is a computer scientist with the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). He launched the center's first health IT use case and, since early 2013, has been overseeing a use case for mobile device security.

Prior to joining the NCCoE in 2012, Mr. O'Brien spent 13 years at NIST's IT Laboratory where he spent much of his time working on healthcare testing tools. While working with groups inside the Nationwide Health Information Network (NwHIN), he also participates as a monitor for the IHE USA North American Connectathon. Before his career with NIST, Mr. O'Brien worked in the startup community during the dot-com era in the mid 90's for a few B2B companies. Mr. O'Brien received a bachelor's of science in mathematics from Bates College and subsequently earned a master's degree in computer science from the University of Tennessee.

William Ash
Strategic Program Manager for the
IEEE Standards Association

According to some studies done by leading firms, nearly $30B to $50B of inefficiencies is attributed to the lack of healthcare data interoperability. Standards provide the mechanism by which to allow data and system interoperability to occur. Standards are also important in exchanging information while protecting privacy. Using standards to allow for a secure and interoperable system would allow for all touch points within the healthcare information and assessment chain to utilize the information in a meaningful way.

His background is in the RFindustry as he worked as applications engineer on wireless communications systems. Bill has been with the IEEE Standards Association (IEEE-SA) for over 12 years working with standards development groups covering technologies such as RF emissions, distributive generation and the National Electrical Safety Code®. He is currently leading the eHealth, smart grid , and smart cities, for the IEEE-SA.

He received his BSEE from Rutgers University School of the Engineering.

Michael Geraghty
Acting Director of Cybersecurity,
Director of the New Jersey
Cybersecurity and Communication
Integration Cell (NJCCIC)

Prior to his appointment, Mr. Geraghty served as Chief Information Security Officer (CISO) of the Hudson's Bay Company, Chief Information Officer of the National Center for Missing and Exploited Children, and Vice President of High Technology Investigations at Prudential Financial.

Previously, he served 12 years with the New Jersey State Police, where he led the formation and development of the High technology Crimes Investigation Unit. He is CIPP Certified.

Engineering Keynote: Setting Expectations with Vendors

Mitchell Parker
Chief Information Security Officer
Temple University Health System

The major issue with third parties these days is vendor communication. Because there haven't been many expectations set on how medical devices need to be operated and maintained in customer environments, it is unclear who is responsible for what aspects of support. Mitch will talk about his experiences in reviewing biomedical products and electronic medical record systems for operational security requirements, and his approach to working with vendors to improve security not only for Temple, but for other customers.

In addition to his role at Temple Health, he is also an adjunct professor in the Information Technology Auditing and Cyber Security program at the Fox School of Business, Temple University, teaching the Cyber Security Capstone. Mitch developed and implemented the information security program at Temple Health, and regularly works with multiple non-technology stakeholders to improve it. He also speaks regularly at multiple conferences and workshops, including HIMSS Privacy and Security, SC Congress NY, and HealthImpact Chicago. Mitch has a Bachelor's degree in Computer Science from Bloomsburg University, a MS in Information Technology Leadership from LaSalle University, and his MBA from Temple University and is CISSP certified.

Healthcare Technical Solutions, llc
Marketing & IT Solutions Supporting Digital Healthcare
Re-Innovating Healthcare

Thank you to Healthcare Technical Solutions

Healthcare Technical Solutions is a marketing communications agency exclusively focused on medical organizations. The company supports growth by attracting new patients, creating loyal advocates from new patients and helping to generate more referrals through existing patients.

"With deep roots in healthcare. We have been working elbow-to-elbow with providers for over a decade with Technology + Marketing + Communications. Our Big, Bold Vision is to achieve the triple aim: reduce patient cost, improve outcomes and improve patient experience."

www.healthcaretechnicalsolutions.com.

Workshop	**Engineering Case Study/Workshop: Security by Design**
Wade Trappe Professor, Dept. of Electrical and Computer Engineering Associate Director, WINLAB Wireless Information Network Laboratory Rutgers, The State University of NJ **Dave Saunders** VP Product Management and Development Galen Surgical Robotics	This short workshop walks the audience through the thought processes associated with identifying and understanding security risks that might exist in medical devices. We will explore potential points of vulnerability, mitigation strategies and how to relate these to other Internet-of-Medical-Things integration capabilities, for attendees seeking cybersecurity management strategies for their own devices. The talk will first examine specific real-world scenario involving surgical robots. With this example as motivation, we will then storyboard a hypothetical IoMT system, called WellMon, intended to support elder care. The audience will be interactively guided through the process of identifying attacks against this synthetic example, as well as outline potential countermeasures that can be applied to enhance WellMon's security. Recently published FDA guidance for Post-Market Management of Cybersecurity in Medical Devices shows that companies must demonstrate a best-effort approach to cybersecurity challenges when designing new medical devices. Developers also need to address and manage vulnerabilities after the product has entered the market. In his talk, Dave Saunders will present details of a surgical robotic system under development and its paths of communication for operation, monitoring, remote service and EMR integration. **Wade Trappe** is a Full Professor of Electrical and Computer Engineering at Rutgers University, a Fellow of the IEEE for his contributions to information and communication security, and Chair of the IEEE Information Forensics and Security Technical Committee. At WINLAB, he directs the lab's research in wireless security. He has led numerous NSF and DoD projects that have resulted in new approaches for securing wireless and sensor networks, and countermeasures that ensure the operational security for tactical networks. Prof. Trappe's research has resulted in over 200 articles and five textbooks on information security. A serial tech sector entrepreneur, **Dave Saunders** has taken over 40 Internet-based products from inception to market since 1991. He has led diverse product development programs including desktop Internet software, access concentration, telco switching, virtual machine clustering and computer-vision-guided surgical tools. An ardent supporter of the Internet of Things, he continues pursuing his vision of a connected world that enriches lives.
	Fireside Chat: The Road Ahead - Pharma/Device Perspectives
Colin Morgan, CISSP, GPEN Global Product Security, Sr. Manager Johnson & Johnson	Colin Morgan is leading the company's Global Product Security initiative to integrate cybersecurity into the Johnson & Johnson product development lifecycle and post market surveillance processes. This effort is focused on developing fundamental cybersecurity policies, standards and processes; establishing integral partnerships with both internal and external organizations; driving education and awareness plans; and monitoring and assessing industry and regulatory trends. He has worked in the cybersecurity field for a number of organizations including the Central Intelligence Agency and the National Oceanic & Atmospheric Administration. He is a featured speaker on cybersecurity and is passionate about the integration of the competency across all industries. Colin holds a Bachelor's degree in Computer Engineering from The College of New Jersey, a Master's degree in Telecommunications from George Mason University, and is CISSP and GPEN certified.
Roberta Hansen Director, Digital Product Cybersecurity Abbott	Roberta Hansen is the Director of Medical Device Cybersecurity in the BTS Organization. Focused on connected medical devices and product software, her group ensures that Abbott pipeline and on market products are designed and developed safely and securely. Roberta began her Abbott career in 1997 as a Project Manager for the Controllership in our Corporate Engineering Division. She led many project and program management roles within Research & Development, Commercial, Supply Chain, Human Resources, and IT Risk Management. Recent FDA Medical Device Regulations paved the way for her governance of medical device design and development and integration with cybersecurity controls. Roberta holds a Masters in Business Administration from Lake Forest Graduate School of Management where she was also Valedictorian. She holds a Bachelor of Arts from The University of Michigan – Ann Arbor in Global Business. She is also holds the Project Management Professional (PMP) designation.

Thank You to All of Our Supporting Speakers, Companies, and Institutions:

Abbott

Alkermes

BioAdvance

Bristol-Myers Squibb

GALEN PARTNERS

IEEE
Advancing Technology for Humanity
ieee.org

Johnson & Johnson

KS

Mallinckrodt Pharmaceuticals

MAYO CLINIC

MERCK

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

OFFICE OF HOMELAND SECURITY & PREPAREDNESS
THE GREAT SEAL OF THE STATE OF NEW JERSEY

ONCONOVA THERAPEUTICS

PRIVACY™ PROFESSOR

SIEMENS Healthcare

Temple University Health System

DEPARTMENT OF HEALTH & HUMAN SERVICES USA
Office for Civil Rights

WINLAB
and Next-Generation Wireless Networking
WINLAB
Rutgers, The State University of New Jersey
www.winlab.rutgers.edu

XYNTEK INC.

ATLANTIC COUNCIL

DataForm SOFTWARE

ERNST & YOUNG

NEW JERSEY INSTITUTE OF TECHNOLOGY
Founded 1881

withum
AUDIT TAX ADVISORY

BRC

BioPharma Research Council
www.biopharmaresearchcouncil.org • 732-403-3137