7:00  Registration / Sponsor / Exhibitor Showcase & Breakfast

8:00  CHAIRPERSON’S OPENING REMARKS AND GREETING
Tim Gee, Connectologist & Principal, Medical Connectivity Consulting

8:15  KEYNOTE ADDRESS: MAPPING PRODUCT TRANSFORMATIONS RESULTING FROM CONNECTIVITY
Medical device connectivity transforms products - often dramatically. Newly connected or interoperable medical devices are used in new and different ways that are often a surprise to both the manufacturer and purchaser. Surprises like this do not bode well for the success and profitability of products, or customers’ satisfaction. This transformation impacts both manufacturers and the health care providers of connected systems because of the new and often unexpected requirements that arise from this transformation. This keynote dissects these transformations dividing them into 6 distinct factors and shows how to use this framework to establish realistic requirements for both products and the necessary services required to install, implement and support connectivity solutions. Manufacturers will benefit from a better methodology for planning and provider organizations will have a tool that can be used to evaluate solutions for purchase, and evaluate manufacturer’s readiness to deliver and support connected and interoperable products. A case study will demonstrate the application of the 6 factors from both the manufacturer and health care provider perspective.
Tim Gee, Connectologist & Principal, Medical Connectivity Consulting

8:45  KEYNOTE PANEL DISCUSSION: PATIENT SAFETY AND HIT
Health IT has promised to bring about great gains in patient safety. However, many new patient safety risks have come to light with HIT adoption and these risks have received high-level attention (e.g., in the national press). Some of these risks have to do with lack of connectivity between HIT systems and medical devices. This panel will discuss the patient safety gains that we expect from HIT and medical device connectivity and the measures healthcare organizations should take to prevent connectivity from becoming a new patient safety burden. Panelists will consider the patient safety aspects of connectivity from a technical, policy, and risk management point-of-view.

9:45  Sponsor / Exhibitor Showcase & Refreshments

10:15  KEYNOTE PANEL DISCUSSION: THE REGULATORY FUTURE FOR HEALTH IT, MOBILE APPLICATIONS, AND INTEROPERABILITY
The Food and Drug Administration Safety Innovation Act (FDASIA) Workgroup is charged with providing expert input on issues and concepts identified by the Food and Drug Administration (FDA), Office of the National Coordinator for Health IT (ONC), and the Federal Communications Commission (FCC) to inform the development of a report on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications that promotes innovation, protects patient safety, and avoids regulatory duplication. This report is expected to be published in January 2014 by the U.S. Health and Human Services Department.

The FDASIA Workgroup is expected to build on prior work such as the Institute of Medicine (IOM) report, Health IT and Patient Safety: Building Safer Systems for Better Care and ONC’s Health IT Patient Safety Action and Surveillance Plan; FDA’s mobile medical applications guidance and Medical Device Data Systems Rule; FCC’s National Broadband plan and other relevant work. Specifically the three agencies will seek input on issues relevant to the report, which include:

- Types of risk that may be posed by health IT that impact patient safety, the likelihood that these risks will be realized, and the impact of these considerations on a risk-based approach;
- Factors or approaches that could be included in a risk-based regulatory approach for health IT to promote innovation and protect patient safety; and

Moderator:
James Keller, Jr., Vice President, Health Technology Evaluation and Safety, ECRI Institute & President, ACCE
Panelists:
Stephen L. Grimes, FACCE, FHIMSS, FAIMBE, Chief Technology Officer, ABM Health
Erin Sparnon, Manager, Health Devices, ECRI Institute
Meghan Dierks, MD, Director of Clinical Systems Analysis, Beth Israel Deaconess Medical Center & Assistant Professor of Medicine, Harvard Medical School
Kathy Kenyon, JD, MA, Senior Policy Analyst, ONC
Medical device systems such as smart infusion pumps are being deployed widely throughout hospitals and becoming more tightly integrated with EMR applications. New classes of systems of systems are also being adopted, such as alarm notification and mHealth chronic disease management systems that are made up of a system of systems, highly interconnected and often dependent on one another for safe and effective operation. Managing risk, providing effective change control and reliable operation on traditional standalone medical device systems was straightforward; the manufacturer took care of almost everything. Systems of systems made up of components purchased over time from separate vendors - and often running on enterprise IT infrastructure - present new challenges as provider organizations shoulder the responsibility to ensure that the various subsystems and components are upgraded or replaced, configured and tested to ensure safe and effective operation of the umbrella system of systems. Systems with these characteristics range from mHealth apps to therapy delivery and patient monitoring. This presentation will introduce evolving best practices for assessing system of systems patient safety risks and managing the never ending component and system upgrades and replacements as these complex IT/medical device systems, and their infrastructure, are supported and maintained over time.

**Jennifer Jackson**, Director of Clinical Engineering & Device Integration, Cedars-Sinai Medical Center

**KEYNOTE ADDRESS: INFORMATION GOVERNANCE - PROMOTE INNOVATION, PURSUE HEALTH IT SAFETY**

ONC has done substantial work in 2013 related to health IT safety, with the clear policy objective of fostering health IT innovation to continually improving health IT safety and use health IT to make care safer. Private sector leadership -- effective information governance -- is key to achieving these objectives. This presentation --

- Calls out the important role of private sector information governance in of ONC’s Health IT Patient Safety Plan
- Urges the need to integrate health IT safety into healthcare “high reliability organizations,” which requires leadership, a culture of safety, and robust process improvement
- Discusses research that identifies high risk, high priority areas for health IT safety – e.g. system interfaces, system configuration, data input, and software functionality – and asks about responsibility.
- Identifies stakeholders who must work together with “shared responsibility” for optimizing the safety and safe use of health IT
- Introduces those aspects of the Safety Assurance Factors for EHR Resilience (SAFER) Guides with the most direct relevance of information governance, including the Organizational Responsibilities SAFER Guide.

**Kathy Kenyon, JD, MA, Senior Policy Analyst, ONC**

**David Classen, MD, MS, Chief Medical Information Officer, Pascal Metrics**

**PLENARY PANEL DISCUSSION: CYBERSECURITY**

Cybersecurity protecting privacy and securing systems from misuse, malicious or otherwise, has become a big topic for medical device connectivity. Whether patient worn insulin pumps, implanted devices like pacemakers, or patient data on smart phones, all computerized and connected medical device technologies are susceptible to cybersecurity threats as has been demonstrated in past white-hat hacker attacks. Regardless of the practicality or likelihood of a
cybersecurity attack on a medical device, the days of waving off cybersecurity requirements because, “no one would do that,” or our device is protected by the obscurity of your proprietary protocol, are fading fast. The FDA’s release of draft guidance on cybersecurity this past summer has signaled manufacturers that FDA is raising the bar on what’s required to digitally secure medical devices for premarket clearance. This panel discussion will explore the cybersecurity issue from the perspective of manufacturers and provider organizations. The FDA draft guidance will be discussed. Specific strategies and tactics for both manufacturers and providers to address cybersecurity will be explored.

Moderator:
Dale Nordenberg, MD, Executive Director & Co-Founder
Medical Device Innovation, Safety and Security
Consortium (MDISS)

Panelists:
Ken Hoyme, Distinguished Scientist, Adventium Labs
D. Mike Ahmadi, CISSP, Global Director Medical Security,
Codenomicon, Ltd.
Brian Fitzgerald, Deputy Director, Division of Electrical and Software Engineering, FDA
Axel Wirth, CPHIMS, CISSP, Distinguished Systems Engineer, Solutions Architect, US Healthcare Industry, Symantec Corporation

3:15 Sponsor / Exhibitor Showcase & Refreshments

3:45 PLENARY PANEL DISCUSSION: INTEROPERABILITY STANDARDS - HOW FAR CAN THEY TAKE US?
Our session will briefly survey the landscape of interoperability standardization—what exists and what is under development—and will highlight both the promise and limitations of that standards work. It will then look at the hurdles and limitations (regulatory, proprietary, legal, technical) that hinder the achievement of full plug & play interoperability. The session will also review the role of hospitals and health systems in the promotion of interoperability.

Moderator:
Joe Lewelling, VP, Emerging Standards, AAMI

Panelists:
Aaron Goldmuntz, MBA, MHSA, Vice President, Business Development & Operations, Center for Medical Interoperability
Julian M. Goldman, MD, Director, MD PnP Program & the CIMIT Program on Interoperability & Medical Director, Partners HealthCare Biomedical Engineering
Shahid Shah, CEO, Netspective

4:45 PLENARY PANEL DISCUSSION: STRATEGIES FOR OVERCOMING ALARM FATIGUE
Alarm Fatigue has a great impact on a hospital’s ability to provide care to their patients. This panel will present the hospital’s perspective from Clinical Engineering and Clinical Leadership on how alarm fatigue is impacting the workflow of the clinician. It will address the challenges created by delivering alarms to the clinician’s wireless device and strategies that the hospitals are using to address these challenges.

Moderator:
Kourtney Govro, MBA, Chief Executive Officer, Sphere 3

Panelists:
Jennifer Jackson, Director of Clinical Engineering & Device Integration, Cedars-Sinai Medical Center
Marni Chandler-Nicoli, RN, MPH, Intensive Medicine Clinical Program Tele-ICU Operations Director/Clinical Program Manager, Intermountain Healthcare

5:45 Day One Concludes; Sponsor/Exhibitor Showcase & Networking Reception
7:30   Sponsor / Exhibitor Showcase & Breakfast

Concurrent Sessions: Choose Either Track A, B or C

TRACK A - WIRELESS COMMUNICATIONS

8:15A   CHAIRPERSON’S OPENING REMARKS  
Shaun Neal, Senior Consultant, Burwood Group

8:30A   PANEL DISCUSSION: BEST PRACTICES TO MANAGE WIRELESS LANDMINES  
Speakers, including experts from AAMI’s Wireless Strategy Task Force (WSTF), will provide specific practical solutions to wireless challenges in the healthcare environment through a discussion of real case studies and practical help with avoiding the landmines. Speakers will highlight the significant wireless challenges in healthcare, help arm attendees with practical tips and tools to avoid the landmines in a wireless environment, and share case studies so attendees can learn from real examples of what works and what doesn’t.

Moderator:  
Shaun Neal, Senior Consultant, Burwood Group

Panelists:  
Bill Saltzstein, Medical Business Development Director, connectBlue  
Tim Rajah, Biomedical Clinical Research Engineer, National Institutes of Health (NIH)  
Olivia Hecht, Field Marketing Manager for Patient Care and Clinical Informatics, Philips Healthcare  
Steven Baker, PhD, Sr. Engineer, Welch Allyn

10:00   Sponsor / Exhibitor Showcase & Refreshments

10:30A   BLUETOOTH AND 802.15.4: KEY CONSIDERATIONS  
Numerous market forces continue to drive the adoption of wireless sensors and other wireless cable replacement technologies. The two technologies receiving the greatest adoption for these applications are Bluetooth and 802.15.4 (including ZigBee). The key issues around these two wireless technologies will be explored from both the manufacturer and health care provider perspectives. Design considerations for building these technologies into medical devices will be discussed. Special focus will be given to managing power consumption and battery life, antenna placement and design, and support for multiple radios. Deployment considerations will be detailed describing best practices on how manufacturers and customers can work together to ensure the timely deployment of reliable wireless systems. On the deployment end, the presentation will address coexistence issues and how they are identified and resolved.

Bill Saltzstein, Medical Business Development Director, connectBlue  
Chris Downey, Product Manager, Laird Technologies

11:15A   THE ECONOMICS OF CONNECTIVITY IN AN ACUTE-CARE ENVIRONMENT  
Connectivity goes beyond the wireless standards and frequency decisions we all must make in our development process. Customers and device vendors look toward a connected future to improve clinical safety and performance and convenience; yet fiscal conditions remain restrictive for the foreseeable future. How can device vendors put forth an economic model that justifies R&D investments to upgrade their devices to a next-generation? We will explore use cases in which device vendors have achieved success in defining and deploying these new economic models, working along with hospitals.  
Amir Jafri, Principal Partner, EVP, Netspective  
Steve Miller, Chief Information Officer, Oklahoma Heart Hospital

12:00A   WIRELESS TECHNOLOGIES AND MEDICAL DEVICE CONNECTIVITY IN THE OR  
The adoption of wireless technologies presents both an opportunity and challenge for the operating room. Most of the equipment in ORs is connected by fiber optic and/or copper twisted cables pulled through boom arms and conduits in the walls, a time consuming, expensive and labor intensive process. Wireless technology has invaded the OR with a wide range of capabilities, improving both the quality of life of patients and doctor-patient efficiency. Wireless technology enables clinicians to monitor patients remotely and give them timely clinical information, reminders, alerts and support – potentially extending the reach of health care by making it available anywhere, anytime. This presentation outlines the advantages of wireless technologies for medical and non-medical devices present in the OR. The presentation will also cover current and future wireless technologies for the OR and the challenges involved with using these technologies. Technologies to be discussed include: Wireless Personal Area Network technologies, WiMAX, Wi-Fi LAN,
Bluetooth, Cellular Technologies (GSM, CDMA-4G LTE, 5G and Zigbee) and WBANs implemented for various medical applications used in the OR environment.

Tim Rajah, Biomedical Clinical Research Engineer, National Institutes of Health (NIH)

12:30A DESIGNING WIRELESS MEDICAL DEVICES FOR THE ACUTE CARE ENVIRONMENT
Hospitals are rapidly updating their wireless network infrastructure to current wireless standards. These standards present both challenge and opportunity while directly impacting the way wireless medical devices connect and communicate critical patient information. In this session, Burwood Group Senior Consultant, Shaun Neal, will cover current best practices, key trends and predictions for hospital wireless networks and discuss their role in the design and implementation of new medical devices and applications. Topics will include the industry shift to the 5GHz spectrum, advanced quality of service and application controls, advancements in security, and the impact of these changes on the medical device and application communities.

Shaun Neal, Senior Consultant, Burwood Group

1:00 Conference Concludes; Luncheon For Attendees Of The Optional Post Conference Workshop

TRACK B - INTEROPERABILITY / SYSTEMS

8:15B CHAIRPERSON’S OPENING REMARKS
Bridget A. Moorman, CCE, President, BMoorman Consulting, LLC

8:30B IHE PCD - A PATH TOWARDS MEDICAL DEVICE INTEROPERABILITY
The session will focus on how the work of the IHE PCD addresses various important clinical use cases concerning the integration of acute point-of-care medical devices with hospital systems. The session will provide:

- An introduction to the topic of medical device interoperability
- Overview of Use Cases and resulting IHE PCD profiles both released and in development
  - Data to EMR
  - Alarms/alerts to alert management systems
  - Point of Care Infusion Management
  - Data from implanted devices
  - Medical Device Security, etc.
- Overview of IHE PCD development process from Call for Proposals to Connectathon and Certification
- Review of guidance provided to HDOs for purchase of products that comply with IHE PCD
- Overview of commercially available complying systems

Ken Fuchs, Executive VP for Interoperability R&D, Center for Medical Interoperability
John J. Garguilo, Computer Scientist, National Institute of Standards and Technology (NIST), Department of Commerce (DoC)

9:15B CHALLENGES TO IMPLEMENTING A STANDARDS INTEGRATED CLINICAL ENVIRONMENT PLATFORM
Medical Device Interoperability is not a new concept but still in its infancy. Understanding the clinical requirements exposes gaps in current state implementing an intelligent interoperability system, the current gaps in standards and approaching other industries haven taken to achieve interoperability. This session will outline the clinical needs, gaps in existing standards and approaches other industries have taken as well as a glimpse of what medical device interoperability could enable.

Tracy Rausch, Founder & CTO, DocBox, Inc.

10:00 Sponsor / Exhibitor Showcase & Refreshments

10:30B HUMAN FACTORS CONSIDERATIONS OF MEDICAL DEVICE CONNECTIVITY
In addition to the extensive technological considerations that influence how medical device may be connected, there are multiple human factors-related considerations. After all, it is healthcare professionals who chose which devices to connect and subsequently employ the functional capabilities and information that arises. Ultimately, to prevent harms, system developers and integrators must perform the necessary analyses to identify use errors that might be induced by the interactive characteristics of connected devices and then implement protections against such use errors. Ideally, the effectiveness of such protections, such as special user interface features, should be validated by means of usability testing.

Michael Wiklund, General Manager – Human Factors Engineering, UL-Wiklund

11:15B EMERGING SAFETY STANDARDS FOR INTEROPERABILITY: UPDATE ON AAMI/UL 2800
Recent regulatory actions have signaled interest in implications of interoperability to system safety. Many standards are now emerging in the medical device/health IT domain to address interoperable component implementations. Where other industries have adopted standards for interoperability, some standards have gone through a full “lifecycle” (from cradle to grave), while others remained and matured; now defining “state of the art.” We will examine the current status of AAMI/UL 2800 and how it proposes to adopt lessons-learned from other industries to satisfy some unmet needs of the healthcare community and its regulators.

Anura S. Fernando, Principal Engineer – Medical Software & Systems Interoperability, Health Sciences, UL Inc.
Traditionally, the performance of medical devices was solely dependent on factors that were under the design and control of the device vendor. V&V would be performed on all electrical, mechanical, algorithmic, and human interface parts of the device and each device vendor would follow their respective quality systems and metrics in order to put forth a safe and approved regulated product. The modern connectivity paradigm has forced a change in this fundamental approach. Whereas the electro-mechanical performance of the device may remain under the control of the device vendor, the algorithmic and human interface elements are many times dependent on the connectivity infrastructure, which not only varies from customer to customer, hallway to hallway, but is completely outside of the device vendor’s control. Therefore, to what level should and could a device vendor push their V&V in order to achieve a comparable level of quality acceptance in the “connected device” future where collaboration with external factors is fundamental for the safe performance of their product.

**Moderator:**
Amir Jafri, Principal Partner, EVP, Netspective

**Panelists:**
Alford R. Taylor, Jr., Director, Division of Electrical and Software Engineering, Office of Science and Engineering Laboratories, Center for Devices and Radiological Health, FDA
David Long, President, Vitech Corporation & President-Elect, International Council on Systems Engineering (INCOSE)
11:15C REQUIREMENTS FOR CREATING AN IT INFRASTRUCTURE TEST ENVIRONMENT
Using IEC 80001-1 as a guide, this interactive session begins with a discussion on determining and mitigating risk. The session will explain why testing should occur; describe how to determine when testing is fruitful, what should be tested, where can testing be done; and provide high-level guidance on how to test IT networks, including what tools to consider for a wireless test lab.

*Steven Baker, PhD, Sr. Engineer, Welch Allyn*

12:00C CONNECTED MEDICAL DEVICES IN THE INTERNET OF THINGS
The next wave of the Internet will connect machines and devices together into functioning, intelligent systems. This “Internet of Things” (IoT) will change every industry, every job, and every home. How will it impact medicine? When?

This talk will reveal how the Internet of Things is changing medicine today by examining real applications of advanced networking technology. The applications include 911 dispatch, EMS transport, imaging, surgery, ICU interoperability, patient safety, hospital integration, and treatment. We will discuss critical needs: finding the right data, delivering high-fidelity waveforms, integrating large hospital systems, ensuring EMR accuracy, and guarding sensitive information.

*Stan Schneider, CEO, RTI*

12:30C SECURITY CONCERNS IN CONNECTED MEDICAL DEVICES FROM BOTH A CUSTOMER'S AND VENDOR'S PERSPECTIVE
How do we manage medical devices that were never expected to be connected or are newly connected to our internal networks and perhaps to the cloud? Integration and interconnected devices and information are the future. But what are the security implications of this new environment? There are new security testing requirements from the FDA. But Fuzz is not enough. What types of threats are out there? Which tools are available to us to find and resolve these issues? Join us for this presentation on the exciting changes in our industry to get answers to these pressing questions.

*John Dougherty, CEO, DSI*

1:00 Conference Concludes; Luncheon For Attendees Of The Optional Post Conference Workshop
With the proliferation of connected health technologies, the need for health information sharing, clinician mobility, new home care models, health data security and privacy are a growing concern. Medical Devices are an integral part of these developments, from increasing integration and networking in the hospital setting to home based patient monitoring. Yet, protecting Medical Devices from cybersecurity threats and assuring the confidentiality and integrity of the data on and transmitted by them is not an easy task. Healthcare providers and device manufacturers are faced with an increasing number of more sophisticated threats, all while highly integrated workflows make us more dependent on the availability of each contributing component. Unlike in other industries, health information is more than just data – it represents a human life. And compromising the confidentiality, integrity or availability of health data and the systems hosting them can not only affect hospital operations, but can impact patient care and in extreme cases health and safety. Corrupt data can lead to diagnostic, treatment, or medication errors and a malfunctioning medical device can harm the patient they are supposed to sustain. This session will bring together medical device and security experts to host an engaging discussion on best practices, balancing the needs for health information security and patient privacy with those of medical information sharing, system integration, and technology adoption.

Example topics to be covered include:

- Evolution of the threat landscape and how it affects medical device security risks.
- Impact of regulations: FDA, HIPAA, and HITECH and what it means for medical device security and privacy.
- From Pacemaker to MRI – different systems, different risks, different solutions. The medical device conundrum – tested for safety and effectiveness, yet a gaping cybersecurity hole.
- Who owns security and privacy anyway? Management, IT, end users, or your clinical engineers?

**Workshop Leader:**
*Axel Wirth, CPHIMS, CISSP, Distinguished Systems Engineer, Solutions Architect, US Healthcare Industry, Symantec Corporation*

**Workshop Instructors:**
*Dennis Seymour, Chief Security Architect, Ellumen, Inc.*
*Deborah Kobza, Executive Director / CEO, National Health ISAC (NH-ISAC), Space Life Sciences Laboratory, NASA/Kennedy Space Center*