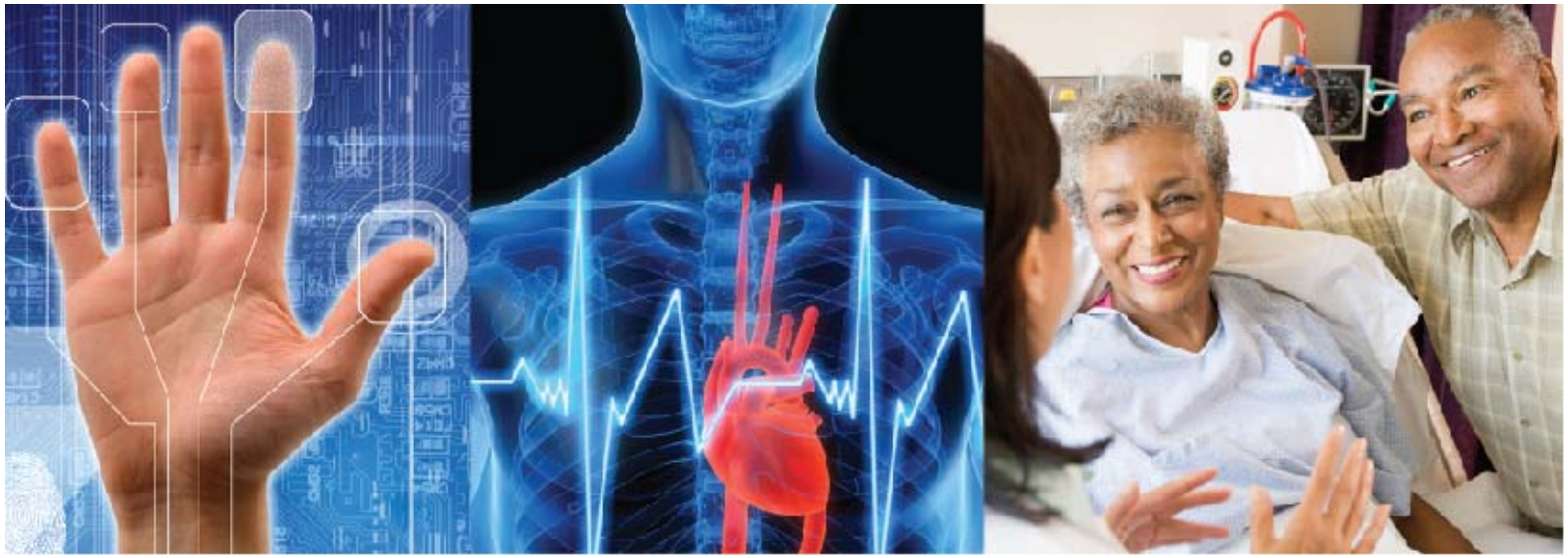
MDISS

Medical Device Innovation, Safety and Security Consortium



Executive Briefing

February 2011

Dale Nordenberg, MD

The MDISS Consortium Provider Advisory Group is co-led by:
VA/VHA and Kaiser Permanent

Medical Device Safety Background

National Biodevice Network
Networked Medical Devices

- Medical devices are a critical component of the nation's health care infrastructure
- Digitally enabled networked medical devices are at risk
  - 'security and privacy' has, for more than a decade, been almost one word
  - 'security and safety' must emerge just as the number and diversity of networked medical devices continues to emerge
- The Medical Device Consortium, established by concerned provider networks, will
  - Build a consortium based on a public-private partnership that enables providers, in collaboration with other key stakeholders, to significantly contribute to the innovation of safe and effective medical devices
  - Determine the scope of medical device safety issues and identify the underlying informatics, public health and engineering challenges
  - Develop the science, data collection networks, and best practices and to secure medical devices towards progressing a safe and innovative biomedical device industry
- The consortium membership will include members from the entire medical device ecosystem including but not limited to
  - Providers, regulators, manufacturers, technology infrastructure companies, academia, patients/patient advocacy groups, standards bodies, and public health agencies

Tip of the Iceberg
Cardiac Implantable Devices Overview

- FDA recalled 23 types of class I implantable products in the first half of 2010
- In 2008, approximately 350,000 pacemakers and 140,000 ICDs were implanted in the United States, according to a forecast on the implantable medical device market published earlier this year.
    - Sanket S. Dhruva et al., Strength of Study Evidence Examined by the FDA in Premarket Approval of CardiovascularDevices, 302 J. Am. Med. Ass'n 2679 (2009).
- Nation-wide demand for all IMDs is projected to increase 8.3 percent annually to $48 billion by 2014 while cardiac implants in the U.S. will increase 7.3 percent annually representing approximately $16.7 billion in 2014
    - Freedonia Group, Cardiac Implants, Rep. Buyer, Sept. 2008, http://www.reportbuyer.com/pharma healthcare/medical devices/cardiac implants.html.
- From 1997 to 2003, approximately 400,000 to 450,000 ICDs were implanted globally, the majority of these implants were done in the USA, and there were at least 212 deaths attributed to failure of these ICDs
    - Robert G. Hauser & Linda Kallinen, Deaths Associated With Implantable Cardioverter Debrillator Failure and Deactiva-tion Reported in the United States Food and Drug Administration Manufacturer and User Facility Device Experience Database, 1 Heart Rhythm 399, t http://www.heartrhythmjournal.com/article/S1547-5271%2804%2900286-3/.

Medical Device Software Failures

- Between 1983 to 1997, 2,792 quality problems that resulted in recalls of medical devices and of problems, 383 were related to device software
- Of the recalled devices, 21 percent were cardiac
- 98 percent of the software failures analyzed were detectable by best practice quality assurance methods
  - Dolores R. Wallace & D. Richard Kuhn, Failure Modes in Medical Device Software: An Analysis of 15 Years of Recall Data, 8 Int'l J. Reliability Quality Safety Eng'g 351 (2001), available at http://csrc.nist.gov/groups/SNS/acts/documents/nal-rqse.pdf.

Infusion Pumps - Software Failure

- Between 2005 and 2009, the FDA received approximately 56,000 infusion pump-related adverse event reports
  - Many of these were associated with significant morbidity and mortality
- Software malfunction was a frequent cause for infusion pump malfunction
- Hundreds of thousands of infusion pumps were recalled and scores of models were implicated
- FDA is providing support to manufacturers
  - Review of code submitted by manufacturers
  - Collaborative development of open source safety models and reference standards
  - White Paper: Infusion Pump Improvement Initiative April 2010, Center for Devices and Radiological Health U.S. Food and Drug Administration, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm205424.htm

Linear Accelerators - Software Related Deaths

- Therac-25 machines
  - Software problems lead to 6 well known cases of death or severe adverse events between 1985-1987 resulting in machine recall
  - Catalyzed safety concerns and resulted in initiatives to improve safety profile of linear accelerators
    - An Investigation of the Therac-25 Accidents, Nancy Leveson, *IEEE Computer*, Vol. 26, No. 7, July 1993, pp. 18-41.
- Radiation related adverse events are likely underestimated
  - Many adverse events are difficult to detect because many are initially subclinical, e.g. increased exposures leading to malignancy
  - "My suspicion is that maybe half of the accidents we don't know about," said Dr. Fred A. Mettler Jr.
    - Radiation Offers New Cures, and Ways to Do Harm, NY Times, January 23, 2010

Risk Reality Check - Hacking Machines vs People

- In 2007 and 2008, health related websites were hacked with the intent to cause harm
  - Coping with Epilepsy website
  - Epilepsy Foundation website
- In both instances, computer animations were posted that triggered migraines and seizures among visitors with epilepsy variants associated with photosensitivity

Hacking of 'medical devices' to intentionally cause harm will occur

ISO Standards
Who in the Healthcare Enterprise Adopts?

- IEC/TR 80002-1:2009(E) provides guidance for the application of the requirements contained in ISO 14971:2007 (Medical devices - Application of risk management to medical devices to medical device software) and references IEC 62304:2006 (Medical device software - Software life cycle)
- IEC/TR 80002-1:2009(E) is aimed at risk management practitioners who need to perform risk management when software is included in the medical device/system, and at software engineers who need to understand how to fulfill the requirements for risk management addressed in ISO 14971
- ISO 14971, recognized worldwide by regulators, is widely acknowledged as the principal standard to use when performing medical device risk management. This technical report may be used to implement a safety risk management process for all software in the healthcare environment independent of whether it is classified as a medical device
- IEC/TR 80002-1:2009 is not intended to be used as the basis of regulatory inspection or certification assessment activities

Reference: IEC/TR 80002-1 – 2009-09 – Technical Report

FDA
Tightening Control to Reduce Risk

- The FDA's Center for Devices and Radiological Health (CDRH) is responsible for regulating medical devices
- Since 1997, the year that the Medical Device Modernization Act (MDMA) was passed, the FDA has encouraged manufacturers to be self monitoring
- The MDMA intention to streamline the approval process has resulted in practices that may increase safety risks
- In August 2010, the FDA working group on medical devices made a series of recommendations to tighten the regulatory approval process for medical devices
- The 510k process will become more stringent and it will be more difficult to claim ‘precedent’ design to justify streamlined approval

Government Oversight - Recent GAO Reports

- GAO report June 2009 identified
  - Gaps in FDA device approval process
  - 510k process is used too liberally
  - Deficiencies in post market surveillance
  - Failure to adequately inspect manufacturers
- GAO reports on VA security Sept 2007, March 2010, May 2010
  - VA responds to GAO sited issues with innovative and effective programs to secure medical devices

Legal Foundations - Medical Device Industry

- Medical Device Safety Act (MDSA) seeks to overturn a 2008 Supreme Court decision that states that manufacturers can't be held at risk for adverse health events due to FDA approved products
- One manufacture's defibrillator was susceptible to breaking and was finally recalled after they were implanted in more than 250,000 patients
- In January 2009, U.S. District Judge Richard H. Kyle in Minneapolis cited the *Riegel* decision to justify the dismissal of over 1,400 lawsuits against this defibrillator manufacturer

Silicon-Based Defects
Etiology of Carbon-Based Diseases

Implanted medical devices have enriched and extended the lives of countless people, but ***device malfunctions and software glitches have become modern `diseases' that will continue to occur***. The failure of manufacturers and the FDA to provide the public with timely, critical information about device performance, malfunctions, and ’fixes' enables potentially defective devices to reach unwary consumers.”

Capitol Hill Hearing Testimony of William H. Maisel,
Director of Beth Israel Deaconess Medical Center,
May 12, 2009

Medical Device Vulnerability
Patient Safety

"These [medical device] infections have the potential to greatly affect the world-class patient care that is expected by our customers. In addition to compromising data and the system, these incidents are also extremely costly to the VA in terms of time and money spent cleansing infected medical *devices*."

Roger Baker

Assistant Secretary for Information and Technology

Department of Veterans Affairs

Medical Device Security Challenges

- The national biomedical device network remains a largely unrecognized entity
- Multidisciplinary expertise is required to understand medical device risks and consequently design, implement, and manage medical devices and their associated biomedical device networks to optimize patient safety
- Stakeholders have not yet built the multidisciplinary expertise required to optimize medical device safety profiles along the medical device life cycle
- Security breaches in the health care industry escalate each year and represent an increasing patient risk as the prevalence of networked medical devices increases
- Medical device security breaches can harm patients and organizations
  - A device's lack of operational effectiveness can directly harm patients
  - Patients' health care information can be compromised and adversely impact care decisions
  - Medical devices can expose an organization's network to further breaches
- Bio-device network dysfunction is a potential national security risk

Medical Device Security Challenges(cont.)

- The security of medical devices, given that they operate as part of a networked system, receive inadequate attention
- Limited information is reported regarding the extent of the potential exposure, risks, and risk mitigation strategies
- Regulatory focus is often about a ‘point in time’ assessment while networked medical devices are continuously exposed to rapidly evolving technology risks
- Collaboration is lacking among all stakeholders (e.g., manufacturers, providers, technology companies and government) to identify the challenges, gather data and promote transparency in developing practical solutions
- The engineering, informatics, and public health science to leverage real-time data streams from networked devices is immature

Consortium

MDISS

Medical Device Innovation, Safety and Security Consortium

Building solutions through collaboration to reduce risk and promote innovation in the U.S. biomedical device network to create a ‘safe medical device industry’

The Consortium - Who We Are

We are a collaborative and inclusive nonprofit professional organization committed to advancing quality health care with a focus on the safety and security of medical devices

We serve providers, payers, manufacturers, universities, government agencies, technology companies, individuals, patients and patient advocates

Mission

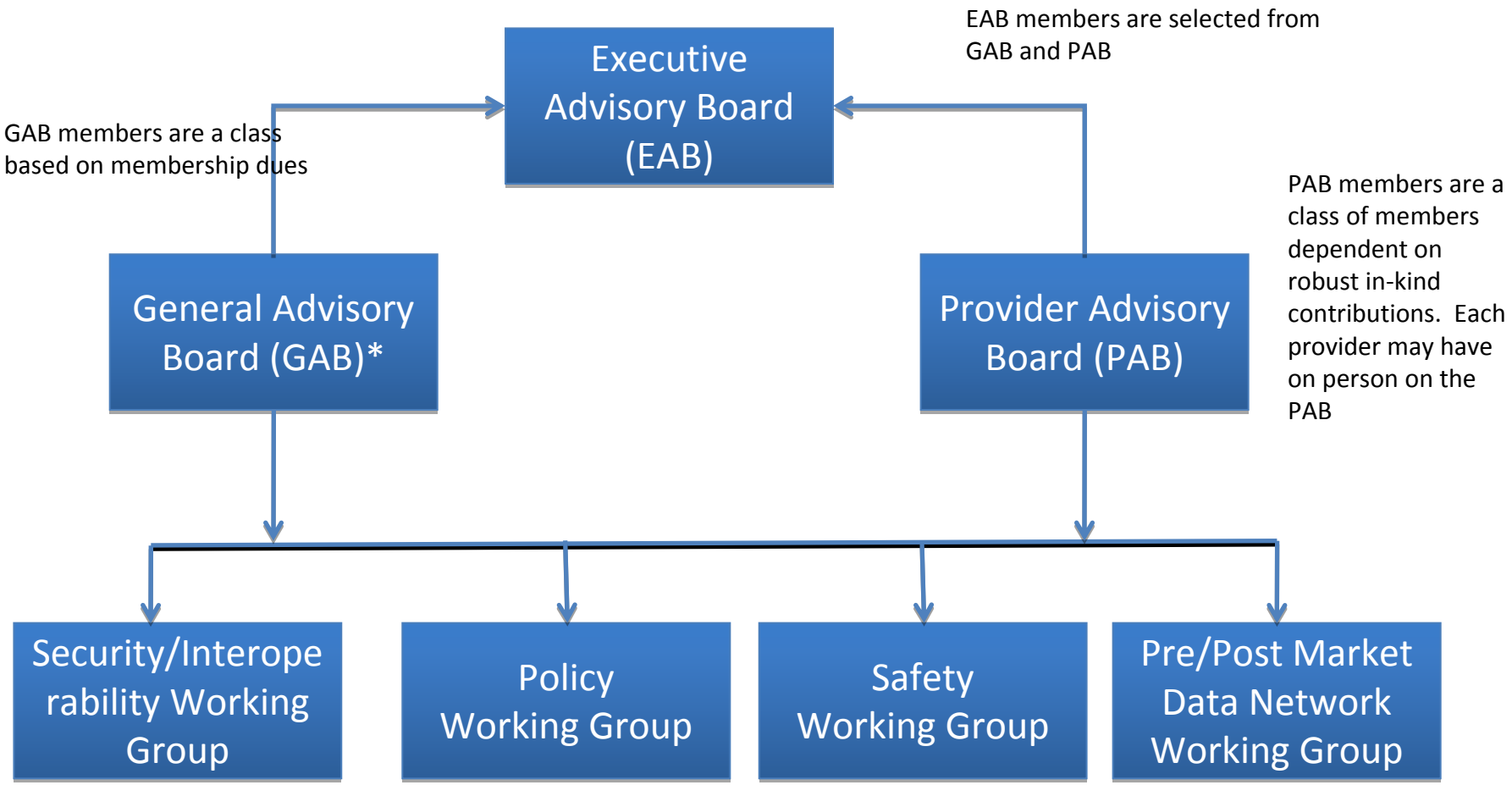
MDISS protects the public's health and well-being by advancing innovation and information risk management practices to ensure wide availability of innovative and safe medical devices

Goal I
Public Private Partnership

A Public Private Partnership Effectively Catalyzes the Development of a Safe, Secure, and Innovative National Bio-device Network

- Build and facilitate a public and private collaborative dedicated to mitigating the risk of medical device associated security and safety risks
- Establish a governance structure to ensure the community serves stakeholder needs
- Establish appropriate working groups/committees to identify and address specific issues
- Ensure representation across government, manufacturers, providers, payers and broader technology companies including infrastructure, security, device components and services companies

Governance Overview



Working groups are co-chaired by GAB and PAB members and are staffed by all member classes
These working groups are provided as examples

Administrative Overview
Organization

- The consortium organization will have the following attributes
  - 501c3 non-profit
  - Consortium will be governed by an executive advisory group
  - Additional advisory groups will support the executive advisory group including:
    - Provider advisory board
    - General advisory board
  - Working groups will be established per advisory group recommendations
- The consortium is funded through membership fees

Establish Working Groups

- Security/Interoperability
  - Create use medical device security cases
  - Identify technical risks
  - Identify technical innovations to mitigate risks
  - Review standards and policy documents, e.g. ISO, and render feedback to appropriate bodies
- Policy
  - Ensuring activities are executed so that they are relevant to and can inform key regulatory issues
  - Liaison with provider accreditation bodies, e.g. Joint Commission,

Establish Working Groups (cont.)

- Safety
  - Develop enterprise-wide (non-silo) cross departmental use cases for medical device risk
  - Develop a comprehensive framework for medical device safety
  - Identify the constellation of risks and conduct root cause analysis for medical device safety issues
  - Ensure organizational dis-integration around medical devices, e.g. IT, biomedical engineering, departmental management, etc. is factored into emerging safety paradigms
- Data networks
  - Development of integrated premarket and post market medical device data collection systems to support clinical trials and adverse event reporting
  - Development of anonymous adverse event reporting for national benchmarking activity

Goal II
Determine the Scope of the Problem

Security Risks Associated with Medical Devices are Well Understood and Appreciated Across the Healthcare System

- Develop case definitions for security risks and medical device associated adverse events
- Develop a data collection network that support premarket clinical trials and postmarket adverse event surveillance
- Establish a public/private reporting infrastructure to accurately assess the national exposure and identify, track and trend incidents
- Ensure the public/private surveillance and adverse incident response model protects the interests of patients, providers, manufacturers and regulators
- Leverage the data collection network to support innovation in medical devices

Goal III
Develop Solutions

Medical Devices and Associated Networks are Safe and Secure

- Develop standards and specifications for how devices are sensed and monitored for adverse events
- Establish best practices for securing legacy medical devices
- Develop a framework and associated practices for managing medical device and bio-device network security
- Establish security standards for the development of new medical devices
- Product white papers that progress the knowledge base for digitally enabled medical device data collection to support pre/postmarket objectives
- Develop training materials

Engineering, Informatics, and Public Health Basic and Translational Science Challenges

- Development of interoperability standards to support medical device communications
- Develop data standards to support communications related to machine operations as well as health care data exchange
- Development of algorithms to monitor device data streams to support detection of malfunction
- Develop hardware, software, and cloud-based solutions to secure networked medical devices against rapidly evolving technology threats
- Develop the epidemiological methods to support medical device adverse event monitoring
- Development of robust data collection networks that leverage real-time data streams from medical devices to support pre-market innovation and post-market adverse event monitoring
- Develop informatics capability to support detection of the association between medical device exposure and healthcare outcomes leveraging emerging EHR infrastructure
- Development of a robust medical device safety science framework supported by effective interoperability standards and real-time medical device communications

Membership Ecosystem

- Providers
- Payers
- Pharmaceutical/OTC manufacturers
- Research organizations, universities, institutes
- Device manufacturers
- Component manufacturers
- Information technology providers
- Information security professionals
- Public sector
- Clinical/Contract Research Organizations (CROs)

Contact:
Dale Nordenberg, MD
dalenordenberg@novasano.com
917-767-1491

Acknowledgments:
The launching and development of MDISS has been made possible by the participation and leadership of the VA/VHA and Kaiser Permanent. In addition to broad leadership and expertise contributions, these institutions are co-leading the Provider Advisory Group.

Kaiser – Patrick Heim, Jing Wang, George Panagiotopoulos
VA/VHA – Jerry Davis, Charlie Gephardt, Megan Friel, Lynette Sherrill