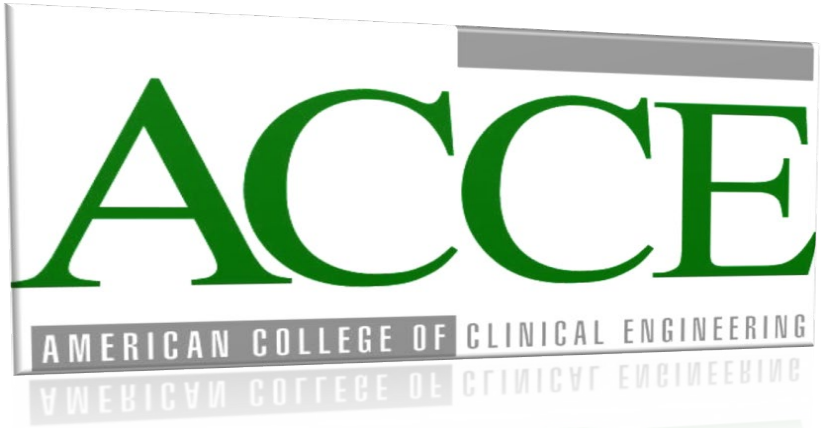


2019 CE-IT Symposium
"Safe and Effective Application of Networked Medical Systems"

Sponsored by

ASIMILY

CloudPost

nuvolo

Zingbox

President's message

Arif Subhan, MS, CCE, CHTM, FACCE
President ACCE
Chief Biomedical Engineer, VA Greater Los Angeles Healthcare System
Adjunct Professor, Biomedical Engineering, University of Connecticut
Member Editorial Boards, JCE, BI&T and 24x7 magazine

ACCE Mission

- To establish a standard of competence and to promote excellence in clinical engineering practice
- To promote safe and effective application of science and technology in patient care
- To define the body of knowledge on which the profession is based
- To represent the professional interests of clinical engineers.

Today's Program

- Safe Networking of Medical Equipment and Systems
- Medical Device Security including Patching of Medical Equipment
- Disaster Recovery Planning
- Emerging Technologies and their Impact on the Hospital Operations
- Long-Term Capital Planning

Medical Device Security including Patching of Medical Equipment

Dr. Julian Goldman
Founder/Director, MD PnP Program
Mass General Hospital
JMGOLDMAN@mgh.harvard.edu

Juuso Leinonen
Senior Project Engineer
ECRI Institute
JLeinonen@ecri.org

Medical Device Security

Considerations for achieving a safe and secure medical device ecosystem

Julian M. Goldman, MD
Anesthesiologist, Mass General Hospital / Harvard Medical School
Medical Director, Partners HealthCare Biomedical Engineering
Director, MGH Program on Medical Device Interoperability & Cybersecurity (MD PnP)

Disclosures: None

Outline

- Why is cybersecurity a unique challenge?
  - Conceptually
  - Technically
  - Clinically
- The relationship between security and interoperability
- The greatest healthcare risk of cybersecurity (hint – it's not technical)
- What can we do today?

Cybersecurity Challenges of Medical Device Systems in contrast to corporate IT systems

- Highly specialized, often unique, systems
  - Network configurations may differ with each vendor and each hospital
- Clinical requirements (such as alarm transmission) may preclude monitoring with Intrusion Detection System technology
- Device s/w version levels, patch levels, configurations are not standardized across the industry and version info typically cannot be read over network
- Networks span a diversity of vendors – regulated and non-regulated
  - Medical device vendors, Integration vendors, IT infrastructure vendors
- Devices as "Black Boxes"
  - Don't have visibility into internal device functions

Understanding the cybersecurity mindset: “best” vs “worst” intentions

- We are patient safety experts – we use best practices to support positive patient outcomes
- Medical device risk-management historically presupposes that use environment contains well-intentioned caregivers
- Cybersecurity is based on attackers with nefarious intent. They exploit weaknesses in systems that were designed to be safely used by those with good intentions.
- Hardening the legacy ecosystem is non-trivial for device manufactures, the FDA, and HDOs
  - Statement from FDA Commissioner: https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm622074.htm

Malware infection of medical device – can it be detected?

- Malware designed for desktop operating systems may exhibit strange behavior on medical devices. Devices may reboot, distort the screen display, or - ??
- If multiple devices in fleet are affected, a high level of suspicion of malware infection is appropriate
- Device failure "cybersecurity-awareness": Swapping devices may not solve the problem! New devices on network may be affected.
  - Manual documentation is basis for "downtime" procedures for EMRs. What is "downtime" procedure for malware-induced "fleet failure"?
    - Ventilator approach – use a self-inflating ventilation bag
    - Will we need to create more equipment-failure backup plans?

Stuxnet "cyberweapon"

- Designed to infect Siemens PLC – programmable logic controllers used for automation.
- Destroyed ~ 1000 gas Uranium enrichment centrifuges (Natanz, Iran)
- Man-in-the-middle attack

"One of the first things this Stuxnet variant does is take steps to hide its tracks, using a trick straight out of Hollywood. Stuxnet records the cascade protection system's sensor values for a period of 21 seconds. Then it replays those 21 seconds in a constant loop during the execution of the attack. In the control room, all appears to be normal, both to human operators and any software-implemented alarm routines."

https://www.theatlantic.com/international/archive/2013/11/stuxnet-used-old-movie-trick-fool-irans-nuclear-program/355340/

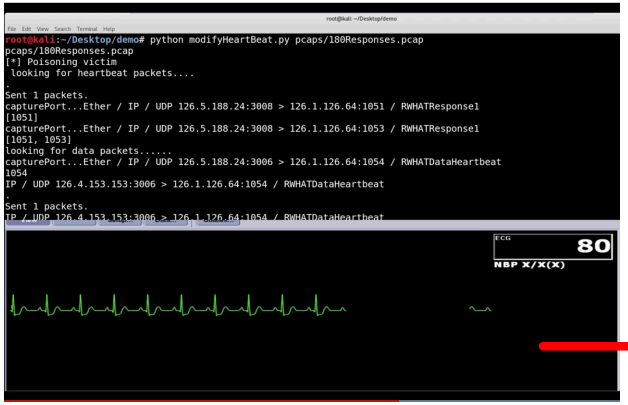
HACKING HL7 DATA INTERFACES IN MEDICAL ENVIRONMENTS: ATTACKING AND DEFENDING THE ACHILLE'S HEEL OF HEALTHCARE

August 24, 2017 Dallas Haselhorst 0 Comment

HL7 non-secured communications are susceptible to man-in-the-middle attack (next slide)

https://www.linuxincluded.com/hl7-medical-attacking-defending/

Modifying ECG Heart Rate value between bedside monitor and nursing central station display



Correct Heart Rate 80

Man-in-the-Middle Attack

Spurious Heart Rate - 180

Experimental setup:

- Nursing Central Station running Windows XP embedded
- Tools – network data sniffer (Wireshark), disassembler
- Medical devices interact with <u>unencrypted</u> UDP communication
- Emulation and real-time injection with ARP (address resolution protocol)

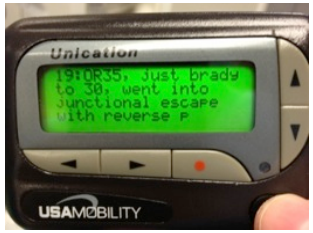
https://securingtomorrow.mcafee.com/mcafee-labs/80-to-0-in-under-5-seconds-falsifying-a-medical-patients-vitals/

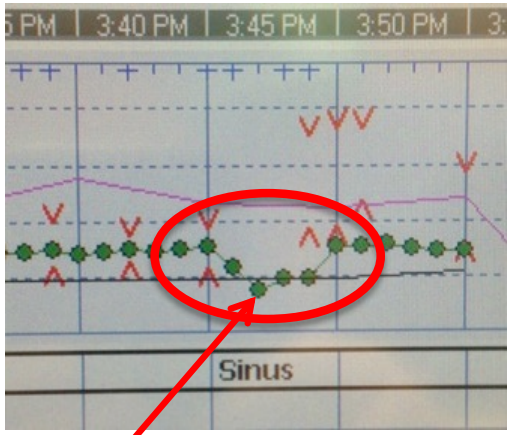
But, what is “normal” device/system behavior?

- Would we know that data is being modified?

Foreseeable Causes of Missing and Spurious data in EHR/EMR

Missed bradycardia in EHR



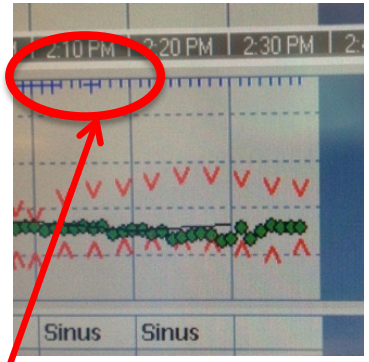


Minimum rate in EHR ~ 45

No evidence of HR=30 in EHR
(Green dots represent HR values)

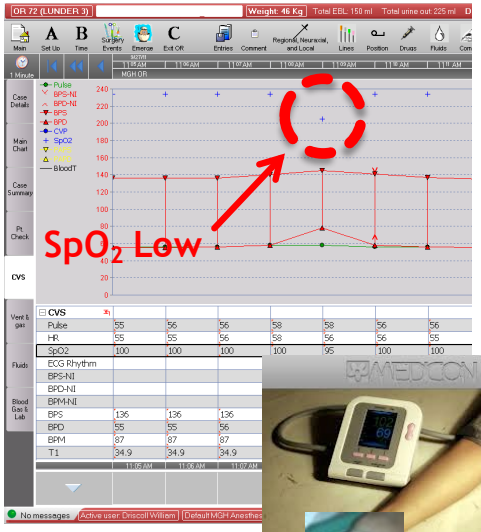
Missing low SpO_2 in EHR

Monitor reveals low SpO_2 "84%" at 2:07



No evidence of SpO_2 = 84% in EHR
(Blue ticks representing SpO_2 value

Falsely low SpO_2 data in EHR



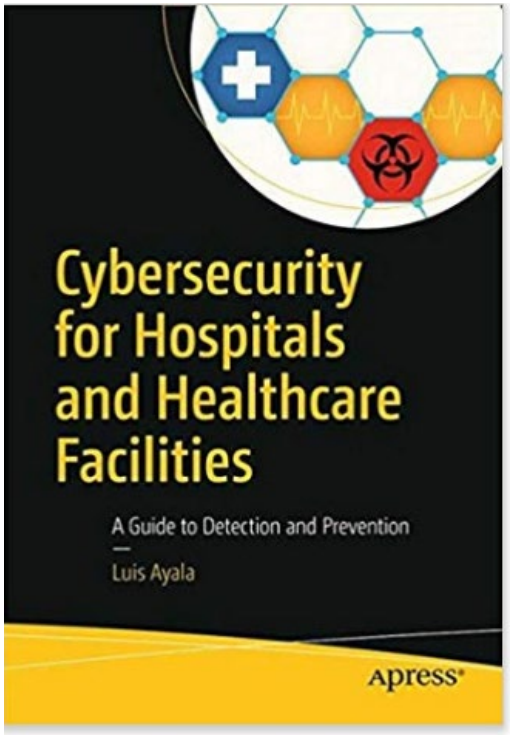
Return of Pulse Ox plethysmogram

Spuriously low SpO_2 in EHR caused by NIBP cuff inflation (Circled in red)

The Need to Apply Medical Device Informatics in Developing Standards for Safe Interoperable Medical Systems (NIHMSID 775190 Publ.ID: AAJ-D-16-01257)

Cybersecurity for Hospitals and Healthcare Facilities

- Speculates on the possible….
- Helps avoid a “failure of imagination”



Luis Ayala, Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention 1st ed. Edition, Apress; 1st ed. edition (September 7, 2016)

Anesthesia Machine

Table 3-7. Possible Anesthetic Machine Cyber-Physical Attacks

Malicious Hacker Activity	Result
Spoof oxygen failure alarm	Ritchie whistle sounds when oxygen pressure is 38 psi (pounds per square inch) descending. Newer machines have an electronic sensor.
Disable Nitrous cut-off or oxygen failure protection device	The nitrous-oxide regulator is a "slave" of the oxygen regulator (i.e., if oxygen pressure is lost then the other gases cannot flow past their regulators).
Disable hypoxic-mixture alarms	Hypoxy guards (ratio controllers) prevent gas mixtures that contain less than 21% to 25% oxygen being delivered to the patient.
Mute all alarms	Anesthetist is unaware of hazardous condition.
Disable interlocks between the vaporizers	Designed to prevent inadvertent administration of more than one volatile agent concurrently.
Change display information	Makes it impossible to monitor the gases and cause confusion as to the flow for oxygen, air and nitrous oxide.
Cause machine to sound random alarms	Interferes with patient procedure.
Interfere with system monitoring the patient's heart rate, ECG, blood pressure, and oxygen saturation	Makes it impossible to monitor the inhaled and exhaled concentration or partial pressure of CO^2 (carbon dioxide), and an indirect monitor of the CO^2 partial pressure in the arterial blood.
Change the dosage doled out to patients	Possible catastrophic consequences (patient not fully anesthetized, overdose medication, drug-drug interactions).
Cause the machine to reboot	Wipes out the configuration settings.

Robotic Surgical Device

Table 3-11. Possible Robotic Surgical Machine Cyber-Physical Attacks

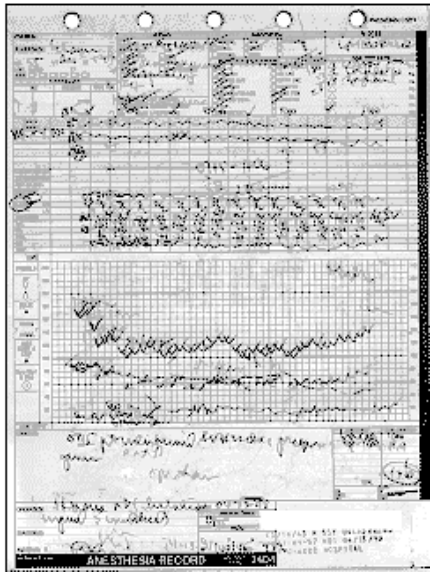
Malicious Hacker Activity	Result
Change display information	Confuses medical laser technician.
Spontaneous reboot	Wipes out the configuration settings. Delay extends the procedure increasing time patient under anesthetic.
Cause machine to sound random alarms	Interferes with patient procedure.
Mute all alarms	Surgeon is unaware of hazardous condition.
Turn off video feed	Surgeon stops the procedure and converts to non-robotic procedure.
Cause uncontrolled movement or arms	Surgeon stops the procedure and converts to non-robotic procedure.
Turn off robot	Surgeon stops the procedure and converts to non-robotic procedure.
Cause network to drop packets	Interferes with patient procedure.

Infusion Pump

Table 3-3. Possible Infusion Pump Cyber-Physical Attacks

Malicious Hacker Activity	Result
Spoof pump with low battery message	Pump ceases to communicate with hospital network.
Override patient pendant button	Pump does not administer pain medication when requested, or provides too much when patient pendant button is pushed.
Spoof pump that door is open	Pump pauses administering medication. Observation should be used to ensure quantity matches—visual verification is needed.
Spoof pump that total dosage was delivered when only partial was done	Patient does not receive full dosage prescribed.
Cause pump to misidentify barcode and download wrong parameters from the drug library for drug being administered	Incorrect autoprogram is administered with incorrect bolus; loading dose, constant fixed-rate, and lockout limit, causes over- or under-infusion, and possibly exceed dose upper limit.
Defeat purge process, alter purge rate	Air may not be removed from the syringe line.
Spoof occlusion pressure	Pump pauses administering medication.
Mute all alarms	Nurse is unaware when pump fails.
Turn off pump, encrypt internal files	Patient does not receive medication. A ransom is demanded to unlock pump files.
Change stored protocols in pump memory	Patient receives incorrect therapy, possibly exceeding dose limit.
Cause pump to prime continuously	Patient does not receive medication.
Change display information	Causes confusion as to what drug was given, what loading dose, and so forth.
Cause pump to sound random alarms	Interferes with patient therapy.
Cause the pump to reboot	Wipes out the configuration settings.

Will cybersecurity issues send us back to the “good old days” (dark ages)?



Hopefully not! Innovation increasingly requires integration of sensors, actuators, and apps.
It is incumbent on us to improve security while increasing data availability and device integration.

Future medical devices and controllers will be increasingly networked to enable autonomous closed-loop care delivery

- Maintaining the security of autonomous medical systems is vital to assure safety
- Remote/virtual and autonomous systems may increase risk exposure by removing a trained operator from the loop

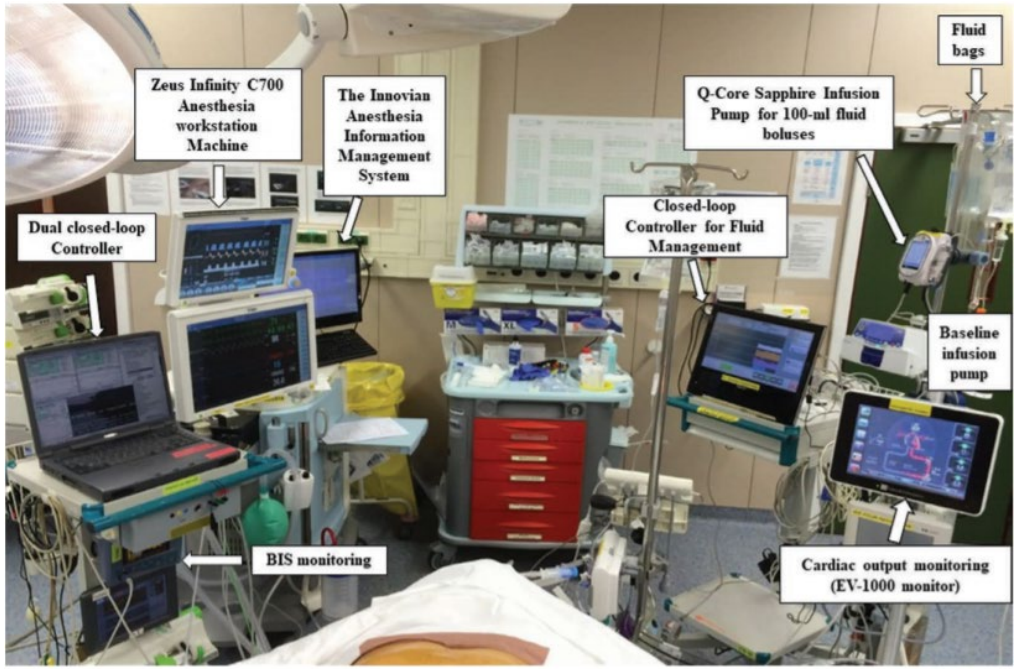
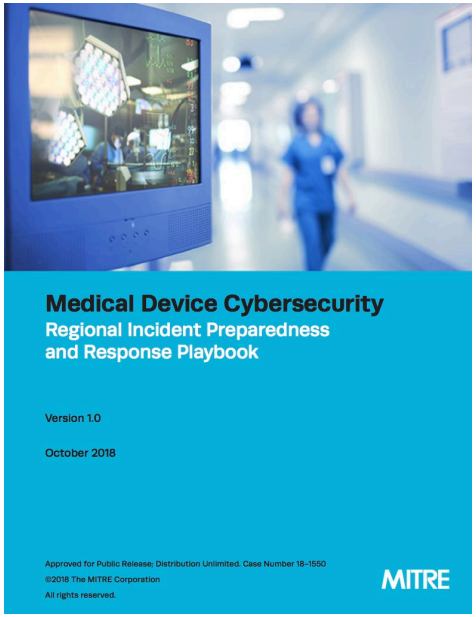


Figure. Closed-loop systems set up in our operating room in Erasme Hospital, Université Libre de Bruxelles, Brussels, Belgium.

Joosten A, Jame V, Alexander B, Chazot T, Liu N, Cannesson M, Rinehart J, Barvais L. Feasibility of Fully Automated Hypnosis, Analgesia, and Fluid Management Using 2 Independent Closed-Loop Systems During Major Vascular Surgery: A Pilot Study. Anesth Analg. 2018 May 9.. [Epub ahead of print]

Regional Healthcare Delivery Organization Medical Device Cybersecurity Workshop – December 2017



- Under FDA support, MITRE and the MD PnP program organized a workshop to
  - Share lessons learned from managing medical devices during the WannaCry attack
  - Identify opportunities to better prepare health systems for future cyber attacks
  - Identify opportunities to improve regional and national sharing
- Brought together IT staff, biomedical engineers, and clinicians from Boston-area hospitals
- Results incorporated in new report: "The Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook " (10/1/18)

https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf

MD PnP Medical Device Cybersecurity Sandbox - *Collaboration between FDA, MITRE, MGH*

Goals:

- The ability to test and validate vulnerabilities, mitigation strategies, and cyber resilient, clinical configurations that enable continued clinical operation in the face of cyber-physical hazards, in support of local, regional, and national preparedness goals.
- A realistic, biomedical environment that supports both preparedness exercises and live cyber-physical incident response activities, with the capability to test solutions in real time.
- The identification and sharing of medical device vulnerabilities, vetted mitigation strategies, and cyber resilient configurations, in direct support of the FDA's postmarket guidance policy calling for greater transparency and adoption of coordinated vulnerability disclosures.

MD PnP
Getting connected for patient safety

MGH 1811 PARTNERS HEALTHCARE

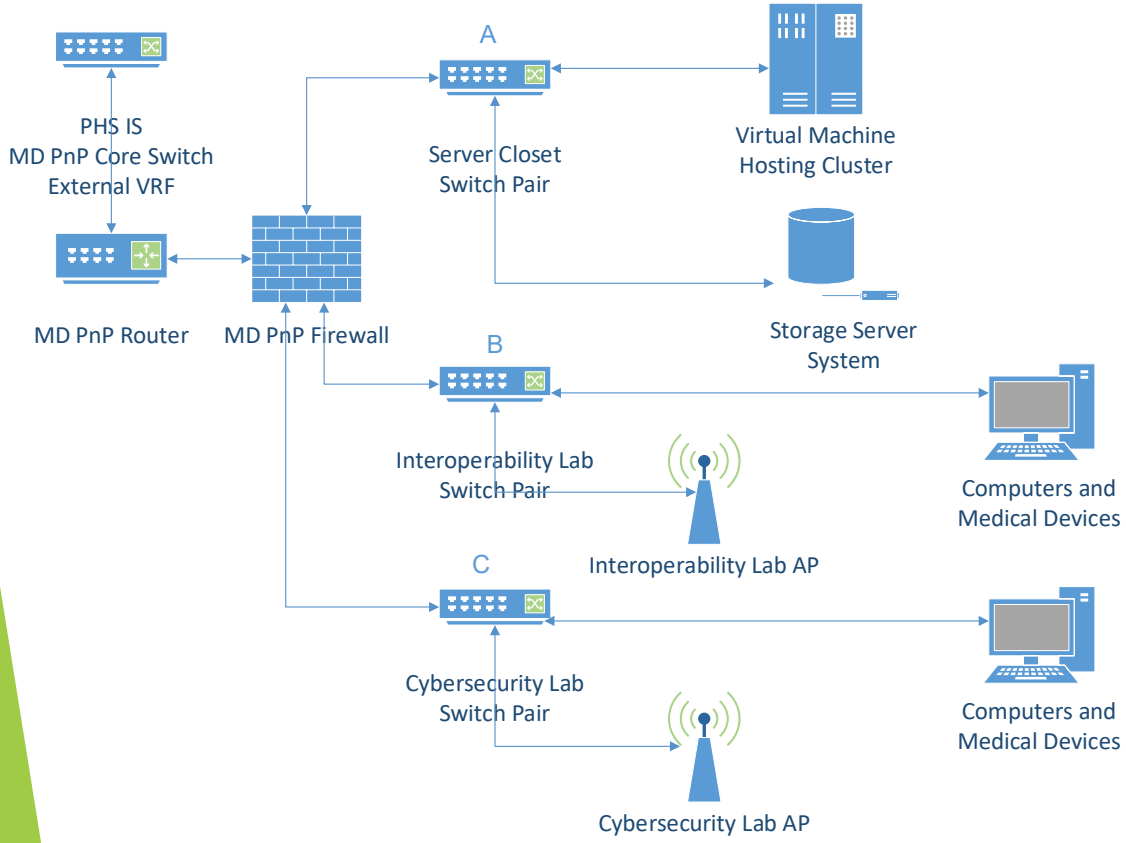
Medical Device Interoperability & Cybersecurity Program
"MD PnP" Lab
65 Landsdowne St., Cambridge, MA

3200 Sq. Ft. Suite contains 4 labs:

- Interop Lab
- Epic BME Integration Lab
- Cyber Lab
- Electronics Lab
- Extensive configurable network environment

Program established 2004. Lab rebuilt 2017

MD PnP Lab Network Architecture



Lab Network Architecture Description

- External VRF – MD PnP router is logically outside of the hospital firewall to minimize risk to operational systems
- Server Closet Switch Pair – VLANs = LAN, Domain Servers (e.g. LDAP), Medical Device Servers, Cybersecurity Servers
- Interoperability Lab Switch Pair – VLANs = Interoperability, Event Hosting, Custom Network 1 and 2
- Cybersecurity Lab Switch Pair – VLANs = Cyber w/ EXT, Cyber w/o EXT, Custom Network 3 and 4

MD PnP™
Getting connected for patient safety™

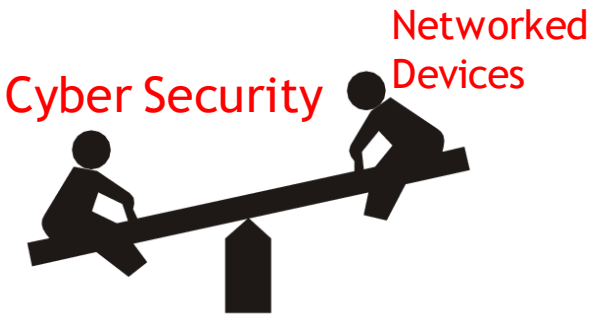
MGH 1811 PARTNERS HEALTHCARE

Current MD PnP Lab Capabilities

- Dedicated DMZs for Research
- External VRF for hosting External Servers
- Dedicated Access Point for Operational Networks
- Dedicated Access Point for Research Networks
- Dedicated Wireless Controller
- Aggregated SPAN port data collection for wired networks
- Ability to integrate and/or access Partners HealthCare network and data center technologies
- Network Packet Inspection Software
- Network Traffic Shaping Software
- Full visibility into all network and server systems
- HardenedBSD Based Router and Firewalls
- Dedicated Managed Switching, Access Points, Wireless Controller
- Custom and dynamically changeable VLANS
- Virtual Machine Hosting Cluster
- Network Authentication
- Multi-Factor VPN Access into Each Network Segment (fine grained control)
- Dedicated Penetration Testing Servers
- Dedicated SPAN data collection ports per network
- Dedicated Data Collection Servers
- Dedicated High Performance Workstations for Penetration Testing and Network Analysis

Lab buildout to support PHS operational projects (pre-procurement assessment) and FDA/MITRE, DHS, and DOD research initiatives

Must we Trade Interoperability for Cybersecurity?



Some say:
"Networked systems increase attack surface and vulnerabilities"
"Close ALL interface ports" (epoxy has been proposed)

Is that possible today?
How would devices be patched? Upgraded?
How would data be integrated? Send data to EHR? Data Dashboard Analytics?

MD PnP™
Getting connected for patient safety™

Relationship between Interoperability and Cybersecurity

VS

- **Like corporate IT networks, next-gen interoperable systems can enable monitoring of device status and behaviors *and* clinical effects of nefarious activity**
- **Cybersecurity requires baselining, data acquisition, and monitoring**
- **Comprehensive, contextually rich data from networked devices enables improved cybersecurity.**
- **Can't monitor devices hidden behind "dongles"**

Comments on the draft guidance are due by March 18th

Contains Nonbinding Recommendations

Draft – Not for Implementation

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on October 18, 2018.

You should submit comments and suggestions regarding this draft document within 150 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions about this document, contact Suzanne Schwartz, Office of the Center Director at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf

Summary

- Most medical device systems are not networked (nor capable of being networked) in a manner that permits the application of modern cybersecurity tools and principles
- We must be vigilant to both protect patients and equipment, and prevent security concerns and solutions from interfering with patient care and inhibiting needed innovation
- Non-networked devices are not necessarily secure
- Start preparing now

What can we do now?

- "Defense in depth" – layers of security, starting with well-designed hospital network that is firewalled from the Internet and segmented (not "flat")
- Maintain good "Cyber Hygiene"
- Build org relationships and processes
  - Consider creating a Medical Device Cybersecurity Response plan (MD-CRP)*
- Vigilance – device misbehavior may be cybersecurity related. Train staff to report.
- Complete device inventory with OS, s/w, patch info
- Safety – prepare for loss of access to device connectivity (e.g. to EHR) or basic functions (blank screen, no output)
- Include cybersecurity requirements in procurement
  - Disclosures, independent testing, standards

* https://www.stahq.org/userfiles/files/044_STA_18AM_Abstract_Goldman%28414%29.pdf

Guidance on Network Segmentation

from the Health Sector Coordinating Council

https://healthsectorcouncil.org/hhs-and-hscc-release-voluntary-cybersecurity-practices-for-the-health-industry/

Compiled by Julian Goldman, MD
February 11, 2019

HHS and HSCC Release Voluntary Cybersecurity Practices for the Health Industry

The Health Sector Coordinating Council (HSCC), in partnership with the U.S. Department of Health and Human Services, is pleased to announce the release of the "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients" publication. The four-volume publication seeks to raise awareness for executives, health care practitioners, providers, and health delivery organizations, such as hospitals. It is applicable to health organizations of all types and sizes across the industry.

This industry-led effort was in response to a mandate of the Cybersecurity Act of 2015 Section 405(d), to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the healthcare industry. The publication marks the culmination of a two-year effort that brought together more than 150 cybersecurity and healthcare experts from industry and the government. The consensus-based document was developed and released under the auspices of the HSCC Joint Cybersecurity Working Group, a public-private partnership to enhance healthcare and public health cyber and critical infrastructure security and resilience.

The publication consists of four volumes:

1. The Main document of the publication explores the five most relevant and current threats to the industry and recommends 10 Cybersecurity Practices to help mitigate these threats.

2. Technical Volume 1 discusses these 10 cybersecurity practices for small healthcare organizations. It is intended for IT and IT security professionals.

3. Technical Volume 2 discusses these 10 cybersecurity practices for medium and large healthcare organizations. It is intended for IT and IT security professionals

4. Resources and Templates provide additional resources and materials that organizations can leverage to develop policies and procedures as well as assess their own cybersecurity posture, through a Cybersecurity Practices Assessment Toolkit.

For more information on this effort and to download a copy of the publication, please visit the 405(d) website at www.phe.gov/405d and https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx.

Health Industry Cybersecurity Practices:

Managing Threats and Protecting Patients

Healthcare & Public Health
Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

6.M.B	Network Segmentation	NIST FRAMEWKORK REF: PR.AC-5

Partitioning networks into security zones is a fundamental method of limiting cyberattacks. These zones can be based on sensitivity of assets within the network (e.g., clinical workstations, general user access, guest networks, medical device networks, building management systems, IoT networks) or standard perimeter segmentations (e.g., DMZ, middleware, application servers, database servers, vendor systems). Examples of standard network zones follow:

- *Perimeter defenses:* Most organizations host services that are accessed through the internet. A robust defense strategy should be deployed to monitor these "front doors."[24]

  Best practices for perimeter defenses include the following:

  - Implement highly restrictive rules on inbound and outbound ports and protocols. Use default-deny rules in firewalls and enable access only when clearly understood.
  - Restrict DMZ from middleware, application, and database servers. DMZ controls are critical, because these servers are exposed to the internet and have a large threat footprint.
  - Restrict the ability for DMZ servers to log in directly to servers on the inside network, specifically using remote desktop protocol, server message block, secure shell (SSH), or other remote access ports (tcp/3389, tcp/445, tcp/139, tcp/22).
  - Ensure that local administrator passwords are unique to each DMZ server and do not use these passwords for any other server in the organization.
  - Ensure that DMZ servers cannot connect directly to the internet. Instead, these servers should access the internet through outbound proxy services. Outbound proxy rules should limit the sites, URLs, IPs, and ports that a DMZ server can access to only whitelisted sites required for updates or application functionality. Be cautious of whitelisting hosting organizations like Amazon Web Services: malicious actors may use them to download malware to a compromised server.
  - Consider this type of restriction configuration for partner WAN links or site-to-site VPN connections. Do not permit access to systems/applications that are not required by the user.

From:

Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

- *Data center networks:* Servers in the data center should be segmented into appropriate zones. Several different layers of segmentation may occur within data center networks, including
  - database servers;
  - application servers; and
  - middleware.
- *Critical IoT assets*: It is important to restrict access to assets that have a potentially high impact on the business or patients if compromised. Management and patching of security vulnerabilities in IoT devices is often limited. Examples include medical devices, security cameras, badge readers, temperature sensors, and building management systems. These assets generally exist outside of the data centers. Without proper segmentation, they may infiltrate general access networks. To achieve segmentation in the physical buildings, leverage multiprotocol label switching to build out virtual networks and place these network access restrictions behind core firewalls.
- *Vendor access:* Vendor access should be limited based on need. It should be temporary, and only access to required information should be granted. Some assets are managed exclusively or accessed by third-party vendors. These vendors may need continual access to the organization's network. It is important to segment this vendor access from other networks and limit the vendor's ability to access other parts of your corporate network. Whether these networks exist inside or outside of the data center, the principles are the same. In 2015, Target was the victim of a cyberattack leveraging these exact channels.[25] Common examples include building management systems, security systems, physical access controls, and persistent tunnels required to enable cloud functionality.
- *General access networks:* The majority of your workforce will operate on general access networks. These are "edge" networks that provide connectivity back to the services offered in data centers, the internet, or other assets. General access networks require a sense of openness when communicating with services that are hosted by the organization. However, restrictions should be implemented that prohibit the assets in one general access network from communicating with the assets in another general access network. This critical control that can help stop the outbreak and spread of malware and ransomware attacks.

- *Guest networks:* It is common for organizations to provide guest access to the internet, especially in provider organizations visited by patients and their friends and families. Access to the internet is a core value of provider organizations. However, it must be restricted and controlled appropriately. These restrictions should exist on wireless networks, where it is most common, as well as wired networks often located in public spaces or conference rooms. Explicitly prohibit access to the internal network; guest users should access the organization

---

25. *Anatomy of the Target data breach: Missed opportunities and lessons learned*. (2015, Feb 2). Retrieved from ZDNet: http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

using the same front door through which they access the rest of the internet. Lastly, as much as possible, limit the ability of your workforce to access guest networks.

About the speaker

Juuso Leinonen
Senior Project Engineer
ECRI Institute
The Discipline of Science. The Integrity of Independence.

- Juuso Leinonen is a Senior Project Engineer at ECRI Institute.
- Manages medical device research/testing projects with published articles on medical device cybersecurity, infusion pumps, and telehealth.
- Investigates medical device problems, hazards, and accidents.
- Developed a standardized process for ECRI Institute medical device security testing and evaluation
- Principal investigator for top 10 Health technology Hazard 2018 Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients
- Volunteer Work:
  - UL 2900-2-1 STP, IHE PCD Planning Committee, ACCE Membership Committee, ACCE Education Committee

Agenda

- ECRI Institute – Cybersecurity as a Top 10 Health Technology Hazard
- Medical device IT and security alerts
- Challenges of patching medical devices
- Recommendations

ECRI Institute

The Discipline of Science. The Integrity of Independence.

- Independent, not-for-profit research institute
- Mission:
  - Improve patient safety, cost effectiveness, and quality of healthcare

"The country's most respected laboratory for testing medical products" – *New York Times*

Multidisciplinary staff composed of: PhD's, MDs, RNs, scientists, engineers, health care professionals

Independent, objective, conflict free expertise

Internationally known as the "Consumer Reports" of healthcare

Over 70% of US hospitals rely on ECRI services

Transforming Healthcare

50 years

ECRI's Top Ten Health Technology Hazards

What it is, and why we do it

- Annual report identifying high-impact health technology hazards

Health technology hazards are device or system faults, design features, or methods of use that might, under certain circumstances, place patients or users at risk

- Produced by ECRI Institute's Health Devices Group to:
  - Shine a light on health technology safety issues that have the clear potential to:
    - Cause death or serious injury
    - Adversely affect patient care
  - Provide healthcare professionals with a tool they can use to:
    - Set patient safety priorities — We Identify topics that we believe warrant attention for the coming year
    - Implement effective changes to help prevent future occurrences

- **2019 - #1. Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare delivery**
- 2018 - #1. Ransomware and Other Cybersecurity Threats
- 2017 - #6. Software Management Gaps Put Patients, and Patient Data, at Risk
- 2016 - #10. Misuse of USB Ports Can Cause Medical Devices to Malfunction
- 2015 - #9. Cybersecurity: Insufficient Protections for Medical Devices and Systems

#1 - Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients

#1 - Ransomware and Other Cybersecurity Threats to Healthcare Delivery Can Endanger Patients

- Ransomware attacks can disrupt healthcare delivery by:
  - Rendering health IT systems unusable
  - Preventing access to patient data and records
  - Affecting the functionality of networked medical devices or disabling third-party services
  - Disrupting the supply chain for drugs and supplies
  - Affecting building and infrastructure systems
- Such disruptions can compromise or delay care

Top 10 Health Technology Hazards 2019

1

Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare Operations

#1 Hackers Can Exploit Remote Access to Systems, Disrupting Healthcare Operations

- Malicious actors are increasingly targeting remote access systems to infiltrate networks
  - Many devices incorporate remote access functionality e.g., PACS
  - Unmaintained systems can be exploited to:
    - Install ransomware or other malware
    - Steal data or render it unusable
- Attacks can severely hinder healthcare operations by:
  - Rendering devices or systems inoperative
  - Degrading their performance
  - Compromising the data they hold

ECRI AlertsTracker - Recall Management System

Accession Number: S0348 **High Priority** Published: Wednesday, April 25, 2018

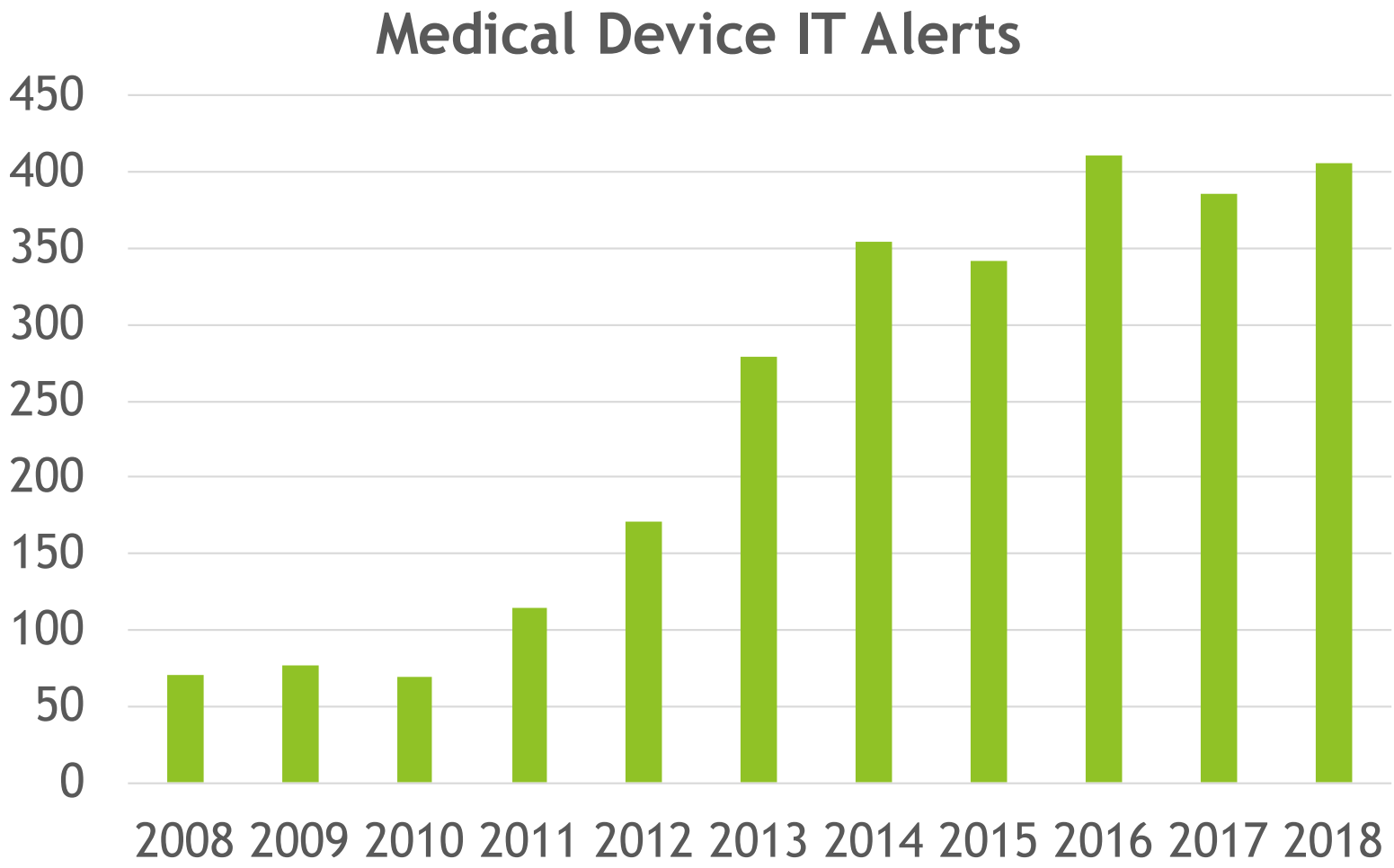
SamSam Ransomware Infections May Affect Care Delivery

Accession Number: S0346 **High Priority** Published: Thursday, April 19, 2018

Ethicon—Gen11 Systems: Software Update May Result in Inability to Use Non-OEM Reprocessed HARMONIC ACE +7 Ultrasonic Devices [ECRI Exclusive User Experience Network]

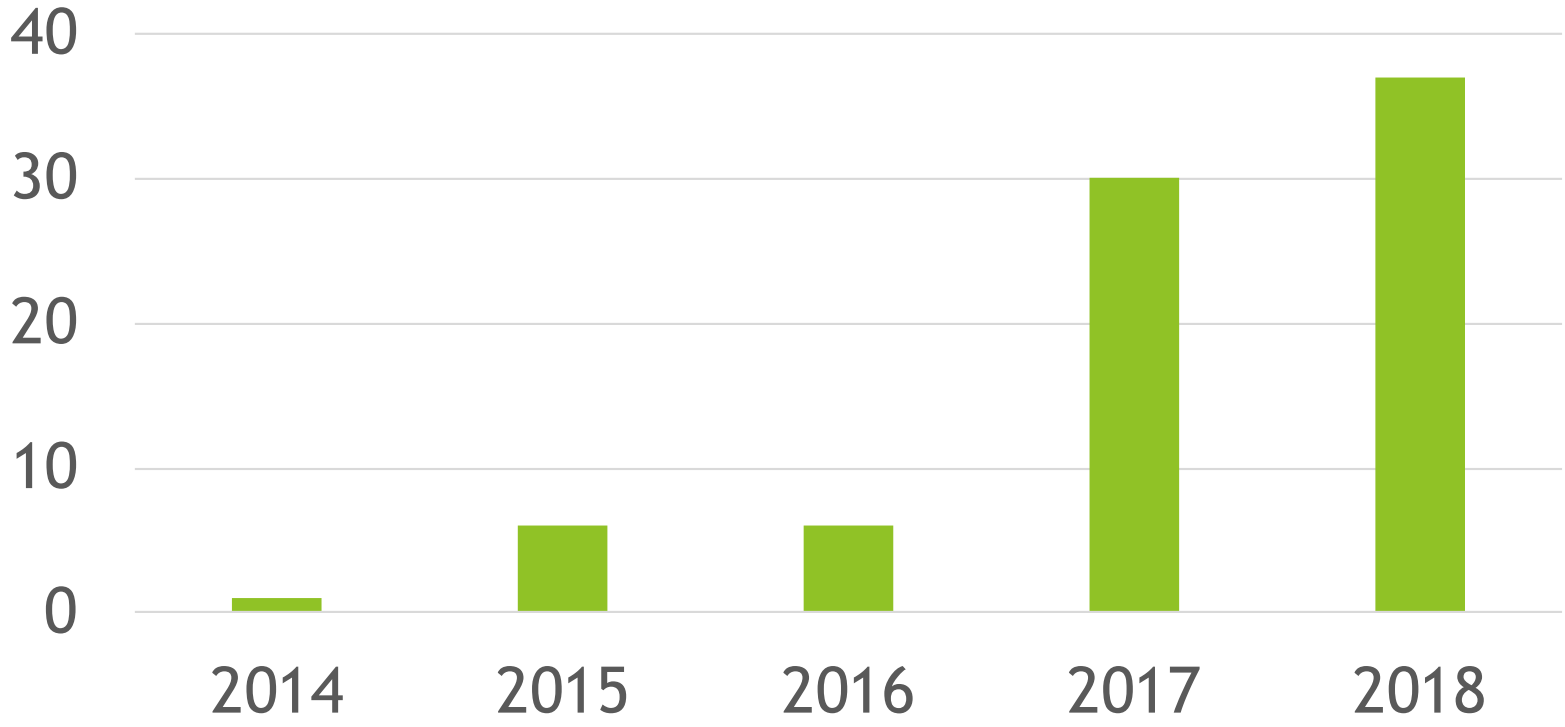
Accession Number: A30432 **High Priority** Published: Tuesday, April 24, 2018

Philips—iSite and IntelliSpace Picture Archiving and Communications Systems: May Exhibit Potential Cybersecurity Vulnerabilities



ECRI Institute – AlertsTracker Database

Medical Device Cybersecurity Alerts



ECRI Institute – AlertsTracker Database

Responding to Security Alerts - Challenges with Patching Medical Devices

- Patching or update often required to respond to a security alert
- Many facilities lack a formal patch management plan and urgent patching strategy

Challenges with Patching Medical Devices

- Impractical to keep systems updated
  - Thousands of medical devices from hundreds of vendors
  - Can directly impact clinical workflow i.e., system downtime
  - Manual updates commonplace
  - May require vendor assistance i.e., Field Service Engineer
- Prioritizing updates
  - How to effectively target limited resources?
- Patch availability
  - Vendor security alert does not mean a fix is available
- Vendors claim that the device software cannot be updated due to FDA requirements

Medical Device Vendor - Challenges with Patching Medical Devices

- Difficulty in getting to the right person within an healthcare facility
  - No great centralized method to communicate about available updates / patches
- Manufacturer information portals require user/customer to actively seek the information
- Software update/patch validation requires significant resources

Recommendations

- Designate a project owner/champion for medical device security alerts
  - May be in Clinical Engineering and/or IT
  - Emerging role of Medical Device Security Specialist

Recommendations

- Establish a process to review and respond to medical device security alerts
  - Where to get the alerts?
    - ICS-CERT, Vendor, ISAOs, ECRI
  - Who to contact with the manufacturer?
    - Establish a list of medical device security contacts
  - How to respond when fix is not available?
    - Identify scalable compensating controls practical for your facility

Questions and Discussions

Disaster Recovery Planning (network recovery)

Sue Wang
Healthcare Sector Technical Lead
National Cybersecurity FFRDC/NCCoE
sue.wang@nist.gov / swang@mitre.org

Chris Nowak, CBET, CHP, CSCS
Senior Director, IT, HTM
Universal Health Services, Inc.
Christopher.Nowak@uhsinc.com

Session Description

- This session will discuss disaster planning for the medical enterprise. The abrupt disruption of all or part of the operations of any business could negatively impact patient care and revenue. Therefore, every business, in order to minimize the negative effects of an abrupt disruption to the business enterprise, a disaster plan is a necessity.

About the speaker:

Sue Wang
Healthcare Sector Technical Lead
National Cybersecurity FFRDC/National Cybersecurity Center of Excellence (NCCoE) at NIST

- Currently the Technical Lead for the Healthcare Sector Team within the National Cybersecurity Federally Funded Research and Development Center (NCF), operated by the MITRE Corporation
- Co-author of multiple cybersecurity guidance publications that offer the healthcare industry detailed instructions for securing electronic health records on mobile devices and wireless infusion pumps in healthcare delivery organizations
- Supported DHS, IARPA and MITRE research projects in software assurance, secure programming, static analysis, and software weaknesses and vulnerability research
- Guest researcher for the Software Assurance Metrics And Tool Evaluation (SAMATE) project at the National Institute of Standards and Technology (NIST)
- Received a bachelor's degree in computer science and a master's degree in software engineering from the University of Maryland

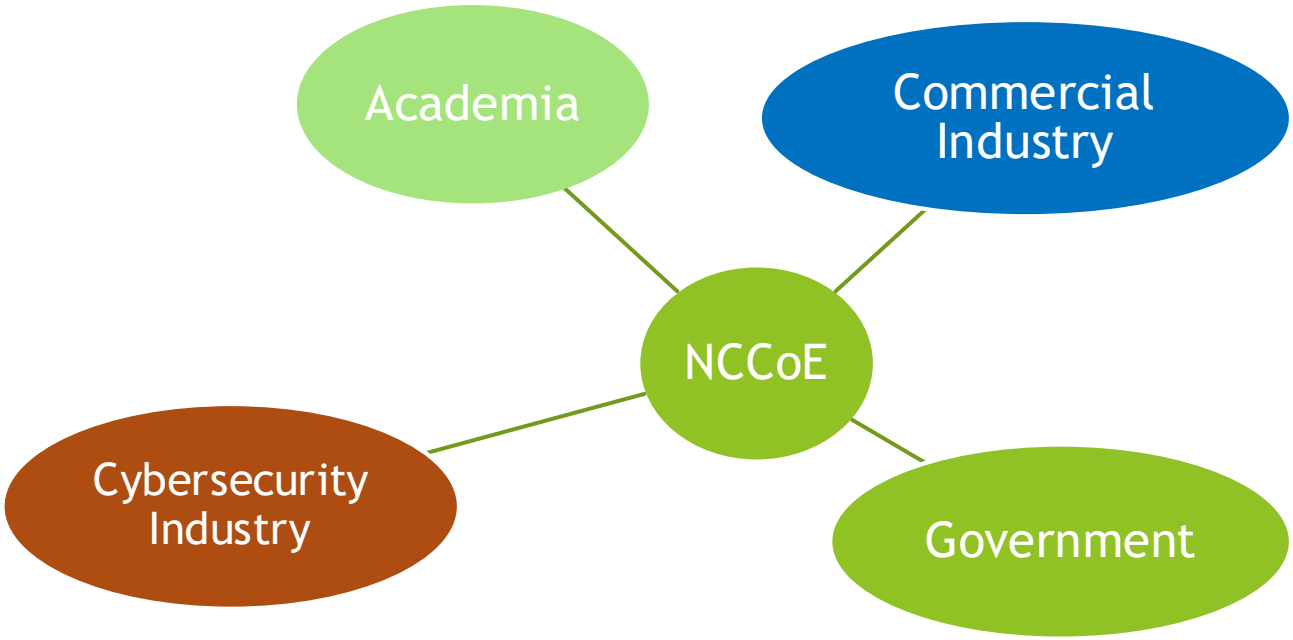
National Cybersecurity Center of Excellence (NCCoE)

https://www.nccoe.nist.gov/

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Collaborative Hub

- The NCCoE works on critical national problems in cybersecurity.
- The NCCoE has access to a wealth of expertise, resources, relationships, and experience.

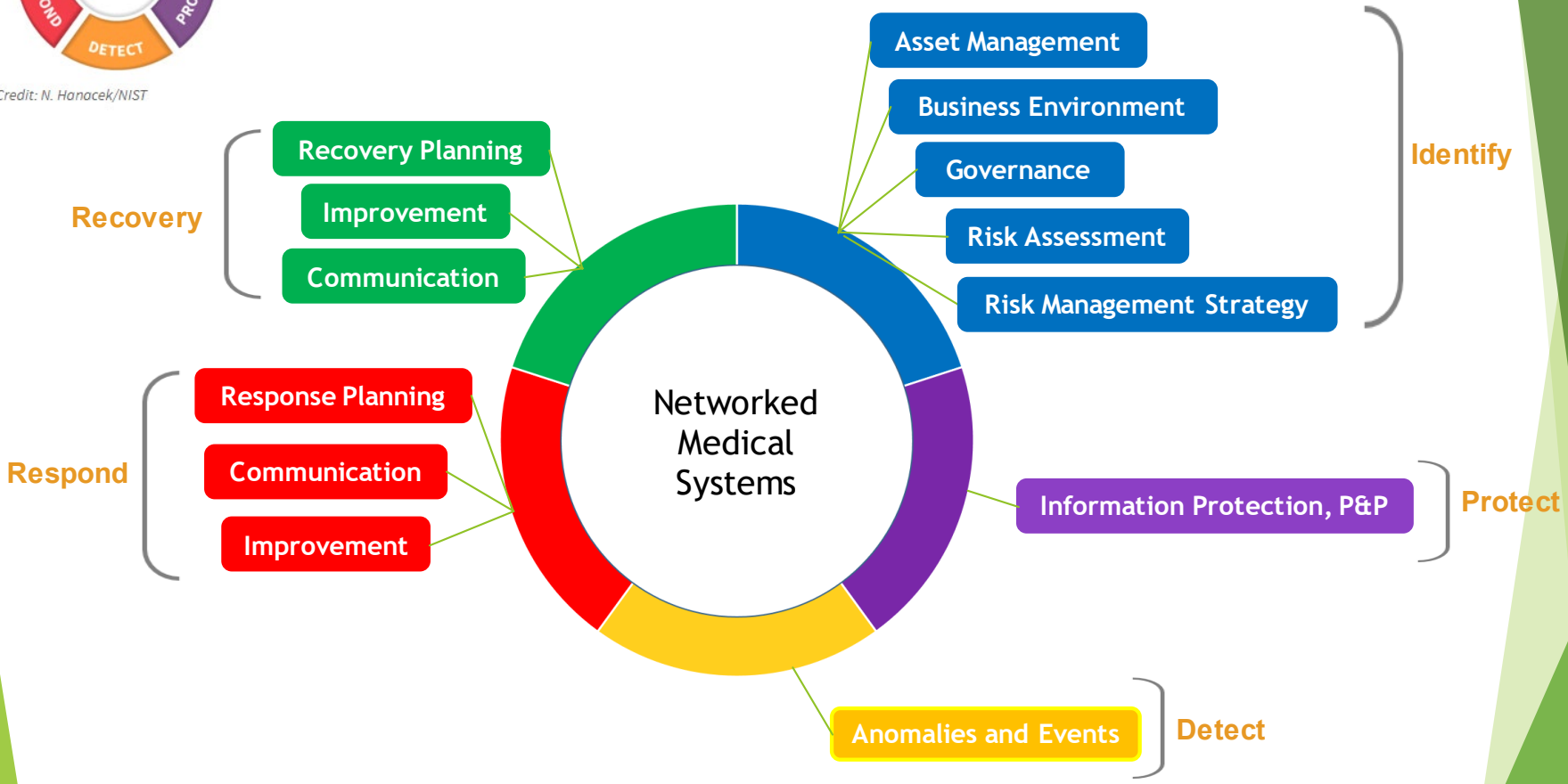


NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Risk Based Approach to Enhance Disaster Recovery and Minimize the Impact of Disruption

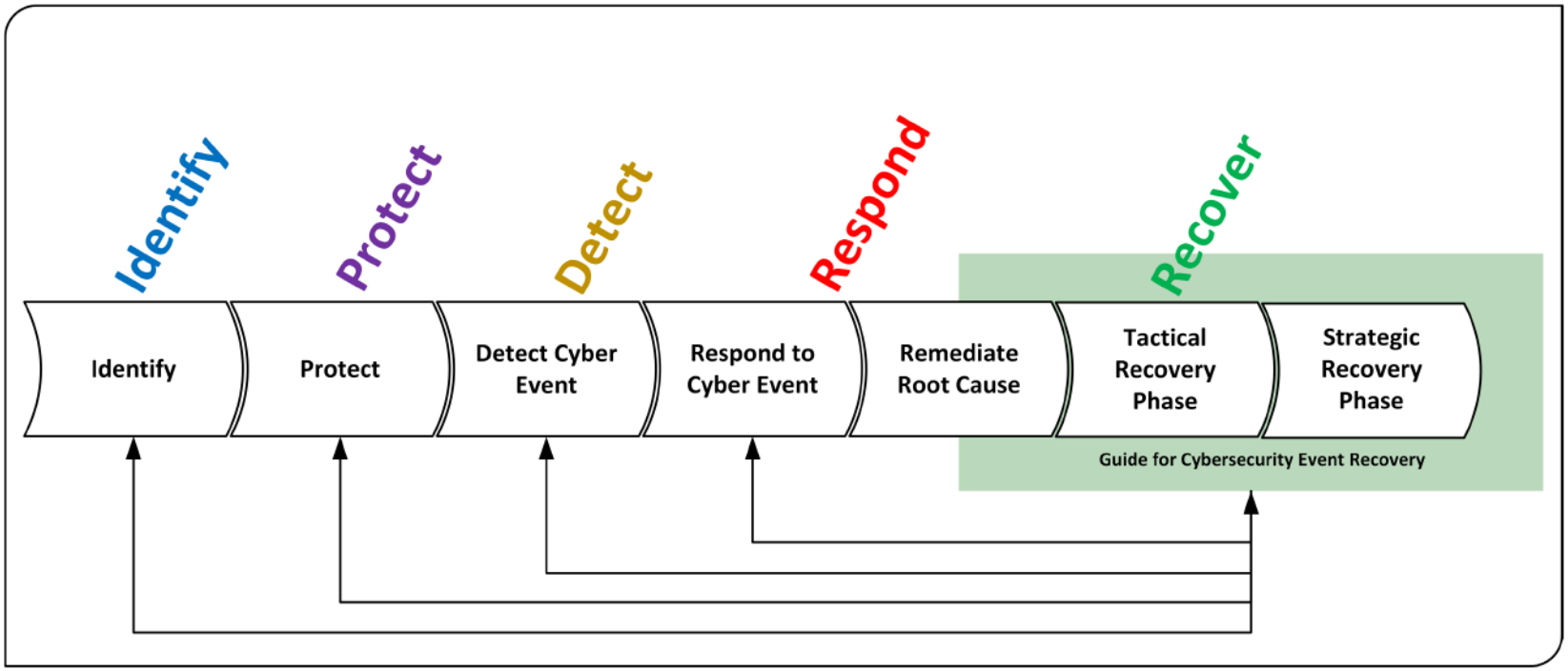
NIST Cybersecurity Framework

Credit: N. Hanacek/NIST



https://www.nist.gov/cyberframework

Improving Recovery & Security Capabilities



Source: NIST SP 800-184 – Guide for Cybersecurity Event Recovery

NCCoE Portfolio

- Attribute Based Access Control (SP 1800-3)
- Consumer/Retail: Multifactor Authentication for e-Commerce
- Data Integrity: Identifying and Protecting
- Data Integrity: Detecting and Responding
- Data Integrity: Recovering (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Email Security (SP 1800-6)
- Energy: Identity and Access Management (SP 1800-2)
- Energy: Situational Awareness (SP 1800-7)
- Financial Services: Access Rights Management (SP 1800-9)
- Financial Services: IT Asset Management (SP 1800-5)
- Healthcare: Securing Electronic Health Records on Mobile Devices (SP 1800-1)
- Healthcare: Securing Wireless Infusion Pumps (SP 1800-8)
- Healthcare: Securing Picture Archiving and Communication Systems (PACS)
- Healthcare: Securing Telehealth Remote Patient Monitoring Ecosystem
- Hospitality: Securing Property Management Systems
- Mitigating IoT-Based DDoS
- Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- Mobile Device Security: Cloud and Hybrid Builds (SP 1800-4)
- Mobile Device Security: Enterprise Builds
- Mobile Threat Catalogue
- Privacy-Enhanced Identity Federation
- Public Safety/First Responder: Mobile Application SSO
- Secure Inter-Domain Routing
- TLS Server Certificate Mgmt
- Transportation: Maritime: Oil & Natural Gas
- Trusted Geolocation in the Cloud (NISTIR 7904)

https://www.nccoe.nist.gov/projects/building-blocks/data-integrity

https://www.nccoe.nist.gov/healthcare

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Relevant Resources for DR

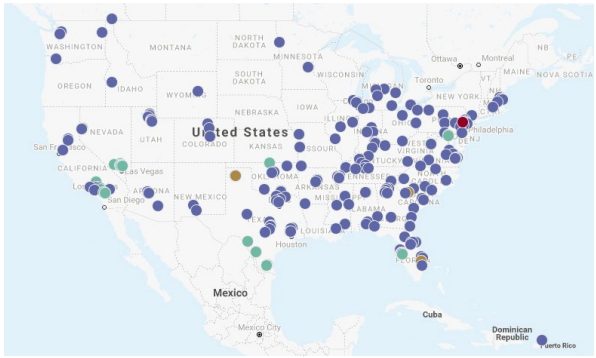
- Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1
- NIST SP 800-184 Guide for Cybersecurity Event Recovery
- NIST SP 800-61 Computer Security Incident Handling Guide
- NIST SP 800-150 Guide to Cyber Threat Information Sharing
- NIST SP 1800-11 DRAFT Data Integrity: Recovering from Ransomware and Other Destructive Events

About the speaker:

Christopher Nowak, CBET, CHP, CSCS
Senior Director, Information Services
Healthcare Technology Management
Universal Health Services, Inc.

- Currently the Healthcare Technology Management Leader responsible for an enterprise-wide program which includes 28 acute care hospitals, free standing emergency departments, imaging centers and clinics across the United States.
- Certified Security Compliance Specialist and Certified HIPAA Professional through ecfirst
- Biomedical Device Integration architect and implementation director
- Responsible for Medical Device Cybersecurity Solutions
- Board Chairman, Association for the Advancement of Medical Instrumentation Credentials Institute (ACI)

About my employer:



- Universal Health Services (UHS), one of the nation's largest hospital management companies, has more than 350 acute care hospitals, behavioral health facilities and ambulatory centers across the U.S., Puerto Rico and the U.K. As we continue to grow, we stay focused on making health a positive and local experience.
- 6,127 Acute Care Hospital Beds
- Independence Physician Management (IPM), a subsidiary of UHS, operates within six states and the District of Columbia through 500+ providers, IPM is dedicated to the support and service of acute care facilities, with limited services for behavioral health. Its focus is on the acquisition, employment and recruitment of independent physicians.
- Publicly traded for-profit healthcare management corporation
- Crossings Healthcare – a software solutions company (https://crossingshealthcaresolutions.com/)


DISASTER MANAGEMENT

Disaster Recovery – Strategy and Planning

- Storms, Fire, Floods, Oh my!
- CYBER ATTACK!
- What constitutes a disaster?
- Small operations vs. large operations
  - Disaster Planning for all
- Predicting the unpredictable
- High Availability vs. Disaster Planning
  - HA – no disruption or continuity of business ops
  - DP – involves downtime, sometimes day, weeks, months, i.e. Nuance $98MM

Disaster Recovery – Strategy and Planning

- What is needed for preparing the DP
  - A complete and solid inventory of hardware and software applications (CMMS)
  - Vendor relationship management
  - Risk rank inventory items
    - Multi-disciplinary team – to define business tolerances for hardware and software applications
    - Risk ranking prioritizes and balances the needs of the caregivers and the business while creating the expectations for the appropriate leadership teams
    - Mission critical apps/hardware
    - Non-mission critical apps/hardware

Equipment Control

Information | History Log | PM Schedule | Information Services | Contracted Service | Expansi

Name Plate

Tag/Asset	158-002169	Manufacturer	TOSHIBA AMERICA MEDICAL SYS
Description	X-RAY,CT	Model	AQUILION PRIME
Type	RADIOGRAPHIC UNIT, COMPUT	Model Name	AQUILION PRIME
Serial No.	30027859	Orig. Manufacturer	TOSHIBA AMERICA MEDICAL SYS

Administration

Building			
Cost Center	CT SCANNER		
Responsible Center	CT SCANNER		
Risk/Inclusion Factor	13		
Location			
as of	03/08/2017	In Service	03/08/2017
Status	Active	as of	03/08/2017

Purchase Information

Supplier	TOSHIBA AMERICA MEDICAL SYS
Ownership	Purchased
Purchase Order	
Purchase Cost	485803.27
Estimated Acquisition Cost	☐

Service Information

Condition	Excellent	as of	01/31/2019
Site ID	30027859		

OK | Previous | Next | Undo | Save

Equipment Control

Information | History Log | PM Schedule | **Information Services** | Contracted Service | Expans

Tag 158-002169 X-RAY,CT

Equipment IT Specs.

Sub-Devices

Device ID	Description	Model	IP Address

Remove Add

OK Previous Next Undo Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169 Maintained By HIPAA Documents

Device | Hardware | Software | Network | Security | Recovery | Location | Support | RTI

Equipment General Details

EIN		Status	Active
Manufacturer	TOSHIBA AMERICA MEDI	Host Name	
Model	AQUILION PRIME	Purchase Date	03/08/2017
Model Name	AQUILION PRIME	Deployment Date	03/08/2017
Serial No.	30027859	Not Applicable	
Type	RADIOGRAPHIC UNIT, CC	End of Useful Life	7
Description	X-RAY,CT	Mfr. End of Life	0
		Purpose/Use	Scan Windows 7 10.191.1.81 Display Windows 7
Available Modules			

Edit

FDA Details

☐ Approved

Approved Date 12/31/2049

Disapproved Date 12/31/2049

Reason

☐ Critical Device

☐ SOX Regulated

☐ PCI Regulated

☐ Computer Based

Close Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169

Maintained By

HIPAA

Documents

Device | **Hardware** | Software | Network | Security | Recovery | Location | Support | RT

Hardware General Specifications

Processor	
Memory (RAM)	
Video Card	
Hard Drive Type	
Hard Drive Size	
ABC ID	
Number of USB Ports	0
USB Ports Speed	
External Storage(s)	
More Details	

Close

Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169

Maintained By

HIPAA

Documents

Device | **Hardware** | Software | Network | Security | Recovery | Location | Support | RT

Hardware General Specifications

Processor

Memory (RAM)

Video Card

Hard Drive Type

Hard Drive Size

ABC ID

Number of USB Ports

USB Ports Speed

External Storage(s)

More Details

1-TB-EPF
1-TB-EPT
2.2
2.53 intel
9.33.1.2
AMD 2.2GHz
CMP-01065
G1820TE
Intel 2.4GHz
Intel 3.2GHz
Intel 3.4GHz
Intel 3GHz
Intel G1820TE
Intel Xeon 5160
Pentium 3.4GHz
XEON 2.6

Close

Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169 Maintained By HIPAA Documents

Device | Hardware | **Software** | Network | Security | Recovery | Location | Support | RT

Operating System

OS Developer
OS Version
License Key
Last Update 12/31/2049
Updated By
Firmware Version
BIOS Version

☐ Firewall Enabled
☐ OEM Restricted
☐ Under OEM Warranty
Warranty
Warranty Exp. Date 12/31/2049
AE Title
DICOM

Installed Software

Save Remove Clear

Version	Software	Install D...	Method

Software
SW Version
Revision Level
Install Date 12/31/2049
Method Used

Close Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169 Maintained By HIPAA Documents

Device | Hardware | Software | **Network** | Security | Recovery | Location | Support | RT

☐ Network Capable ☐ Connected to Network Domain Name Router Details

Wireless Network

Network Model
Network Type
Network Drop Location
IP Address Type ◉ DHCP ○ Static
IP Address v4
IP Address v6
Subnet Mask
Default Gateway
MAC Address
Frequency
Edit

Connected to ☐ WAN ☐ Internet ☐ Intranet ☐ VLAN ☐ LAN ☐ VPN

Wired Network

Domain Work Group
Network Type
Network Drop Location
IP Address Type ◉ DHCP ○ Static
IP Address v4
IP Address v6
Subnet Mask
Default Gateway
MAC Address
Port
DNS

Connected to ☐ WAN ☐ Internet ☐ Intranet ☐ VLAN ☐ LAN ☐ VPN

Close Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169

Maintained By

HIPAA

Documents

Device | Hardware | Software | Network | **Security** | Recovery | Location | Support | RT

Wi-Fi Details

Wi-Fi MAC Address

SSID

Password

Serial Number

Frequency Band

Channel Widths

Signal Stream

Router Location

Router IP Address

Router Username

Router Password

Protocols

Other

Firewall

Bluetooth Passkey

USB Port Password

☐ USB Lock

☐ Ethernet Port Secured

Antivirus

Antivirus

Antivirus Version

Last Update 12/31/2049

☐ Auto Update Antivirus

Close

Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169

Maintained By

HIPAA

Documents

Device | Hardware | Software | Network | Security | **Recovery** | Location | Support | RT

Last Backup	12/31/2049
Next Planned Backup	12/31/2049
Backup Method	
Backup Schedule	
Recovery Point Objective	
Recovery Time Objective	
Priority of Recovery	
Storage Method	

Close

Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169

Maintained By

HIPAA

Documents

Device | Hardware | Software | Network | Security | Recovery | **Location** | Support | RT

Building Name

Floor Number

Room Number

Location Detail

Building Addr.

City

State

Zip

Region

Service Area

Close

Save

Equipment IT Specifications -- Webpage Dialog

Tag 158-002169 Maintained By HIPAA Documents

Device | Hardware | Software | Network | Security | Recovery | Location | **Support** | RT

Support History

Save Remove Clear

Service Software	Update ...	Vendor

Support Details

Vendor

Update Date 12/31/2049

Service Software

Version

Method Used

Cost if Fee

Critical Updates

Add

Remove

Close

HIPAA -- Webpage Dialog

HIPAA	Capability	Used
Store/Transmit ePHI	☐	☐
Logon Compliance	☐	☐
Password Compliance	☐	☐
Auto Logoff	☐	☐
Encryption	☐	☐
Audit	☐	☐

Cancel OK

Disaster Recovery – Strategy and Planning

- Responsibilities – key roles and the parties that need to be involved.
  - Who declares the disaster?
  - Roles for the C-Suite all the way down through the organization are defined and understand the processes of the DR plan.
  - Who's who listing and their roles and contact information
  - Depth to the plan – Roles defined to the extent of "back-up" staff in the event of vacation or the inability of the primary role to fulfill obligations.

Disaster Recovery – Strategy and Planning

- DR Communications
  - Plan for the worst! Do not assume that telecommunications or network operations (ip phones/e-mail/text) would be available
  - Written plans in place for not only internal staff/employees but also external vendors, suppliers and emergency personnel.

Disaster Recovery – Strategy and Planning

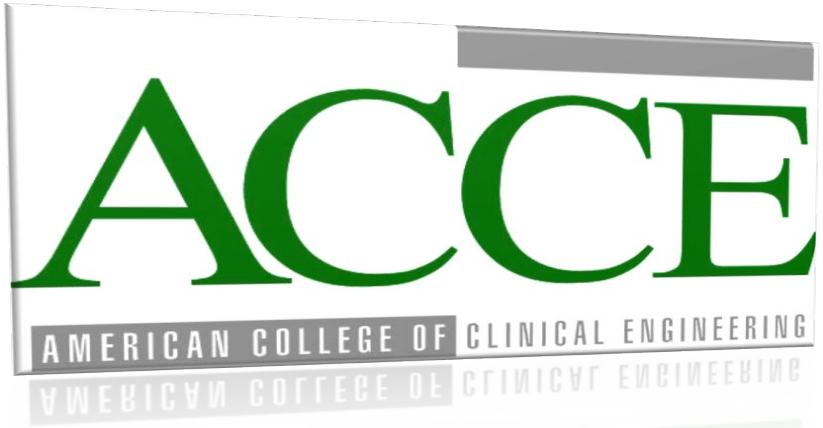
- SLA's – strong definition of services in the event of a disaster
  - Performance defined with penalties
  - Hidden fees?

- Continuous Maintenance
  - Be cognizant of changes within the business – new applications, retired applications, hardware needs, communication plans and human capital changes.
  - Plan Ownership

Disaster Recovery – Strategy and Planning

- TEST, TEST, and TEST!!!!!
  - If you are not testing your plan, then you don't really have a plan.
  - How often?
  - How comprehensive?
    - Consider testing the plan in subsets to meet desired frequency and completeness as the business can tolerate
  - Checklists
  - Impact of staff turn-over – test your employees
  - Include your vendors in any testing strategies

Questions and Discussions



Safe Networking of Medical Equipment and Systems

L Michael Fraai, MS, CCE
Executive Director: Biomedical Engineering & Device Integration
Brigham and Women's Hospital

Bridget Moorman, CCE
President
Bmoorman Consulting, LLC

HIMSS 2019: CE-IT Symposium
"Safe Networking of Medical Systems"

L Michael Fraai, MS, CCE
Executive Director: Biomedical Engineering & Device Integration

BRIGHAM HEALTH
BRIGHAM AND WOMEN'S HOSPITAL

About the speaker

L. Michael Fraai
Executive Director – Biomedical Engineering & Device Integration
Brigham and Women's Hospital

Michael, a native of Curaçao, has an Undergraduate Degree in Biomedical Engineering from Tulane University, New Orleans, LA and a Graduate Degree from the Hartford Graduate Center/RPI, Hartford, CT.

Michael joined the Brigham and Women's Hospital in 1994 as a Clinical Engineer. In 1997 he was promoted to Assistant Director of Biomedical Engineering then in 2002 he was offered the role of Director. Most recently in 2014 Michael was promoted to the position of Executive Director of Biomedical Engineering & Device Integration.

Michael focuses on strategic & innovative use of technology to match the current clinical practice model in the hospital.

Michael is responsible for implementing a hospital- wide telemetry system, a patient care network of 1000+ devices and maintaining an inventory of 24,000+ medical devices covering the BWH's distributed campus.

Brigham Health

- National leadership in patient care, quality improvement and patient safety initiatives, and its dedication to research, innovation, community engagement, educating and training
- Brigham and Women's Hospital (BWH) employs ~16,000 people; 3,000 physicians, fellows and residents; more than 1,000 researchers and 3,113 nurses
- In 2011, performed the first full face transplantation in the US
- Inpatient admissions totaled approximately 46,000
- Biomedical Engineering supports ~26,000 patient care devices
- BWH went live on 05/30/15 with one of the largest EHR installations in the US that included Biomedical device integration (BMDI)

- 793 licensed beds
  - 146 ICU beds
- Patient care network ~ 1600 devices
  - 489 Telemetry beds
  - 43 Operating rooms
- BMDI integrated into EHR system
  - ~1900 devices

Agenda

- Medical systems & Safe Networking
- Methodology
- Devices connected on the IS network
- Dedicated Patient Care/ Vendor Networks
- The process
- Lessons learned

Partners eCare Goals

- One Patient, One record, One Team and One Partners Statement
- Consistent, standardized processes
- One system integrated across the enterprise
  - 2 Academic Medical Centers
  - 17 Community hospitals
- Safe networking of medical systems becomes critical
  - The importance of architecture and configuration for security
    - Across entity
    - Across system

Safe Networking of Medical Systems

- Devices connected directly on the IS network
  - Hardwire
  - Wireless
- Dedicated Patient care networks interfaced to an IS network
  - Devices that are connected on a dedicated network which interfaces to the IS network
- Physical security of networks
  - Access to network infrastructure i.e. closets
- Network Security configuration

Methodology used

- Develop clinical and technical requirements for security, redundancy and uptime
- Collaborate with your IS department
- SMDZ (Safe Medical Device Zone) configured on the IS network
- Configure routers
- Vendor configuration on the networked devices to ↑ security and limit access
- Involve vendors and hold them accountable to meet the current security standards especially for your institution/enterprise
- Network monitoring/ management tools

Directly connected devices on your IS network

- Examples include:
  - RFid systems
  - ECG archival systems
  - Patient access ultrasound devices
- Collaborate with your IS department to understand the requirements before purchase and connection
- Often vendor submission documents are used
  - (Partners Vendor Information Security Plan (VISP)

a. Access Control

<Describe the technical, operational, and management controls used to provision access to systems and data. Include how user accounts, privileged access, and access to data (i.e. least privileges, access roles, permission) are managed for an employee over time. Include access authorization, management approval, access reviews. This should include both the vendor's internal security practices and application design (where applicable).>

b. Identification and Authentication

<Describe the organization's identity and authentication policy, standards and procedures, including how users access Partners Services, Systems, data and how those users are identified and authenticated. Examples include unique user accounts, password configuration and policy enforcement, federated identity management, 2-factor authentication.>

c. Awareness and Training

<Describe organizational requirements related to workforce information security awareness and training, including how employees are trained on securing devices, accounts, applications, services and data.>

d. Audit and Accountability

<Describe organizational requirements related to audit information, including what events are audited, the retention of audit information (i.e. how long are they retained, are they protected), and monitoring and auditing for unauthorized information disclosure. Describe what information is captured in audits and logs such as name, user ID, date and timestamp, access activity details.>

e. Certification, Accreditation, Security and Risk Assessments

<Describe how the organization certifies the information systems used for the solution are secure. Also, describe how the organization certifies the computing environments of subcontractors. Examples include SOC 2 Type 2 audits, other audit and certification activities, vulnerability scanning, penetration testing, internal review procedures. Also, describe the organization's approach for assessing risk, including whether formal risk analysis are performed, and whether vulnerability assessments and penetration testing are performed for the information technology resources used for the solution.>

f. System and Communications Protection

<Describe the organization's communication security policies, standards and procedures, including the organization's secure transmission capabilities, and how the organization secures the information technology resources from external threats. This section should also describe the controls implemented to secure data and documentation as it is transmitted over untrusted networks (e.g., the internet). Examples include network perimeter security, intrusion detection, encryption of data-in-transit.>

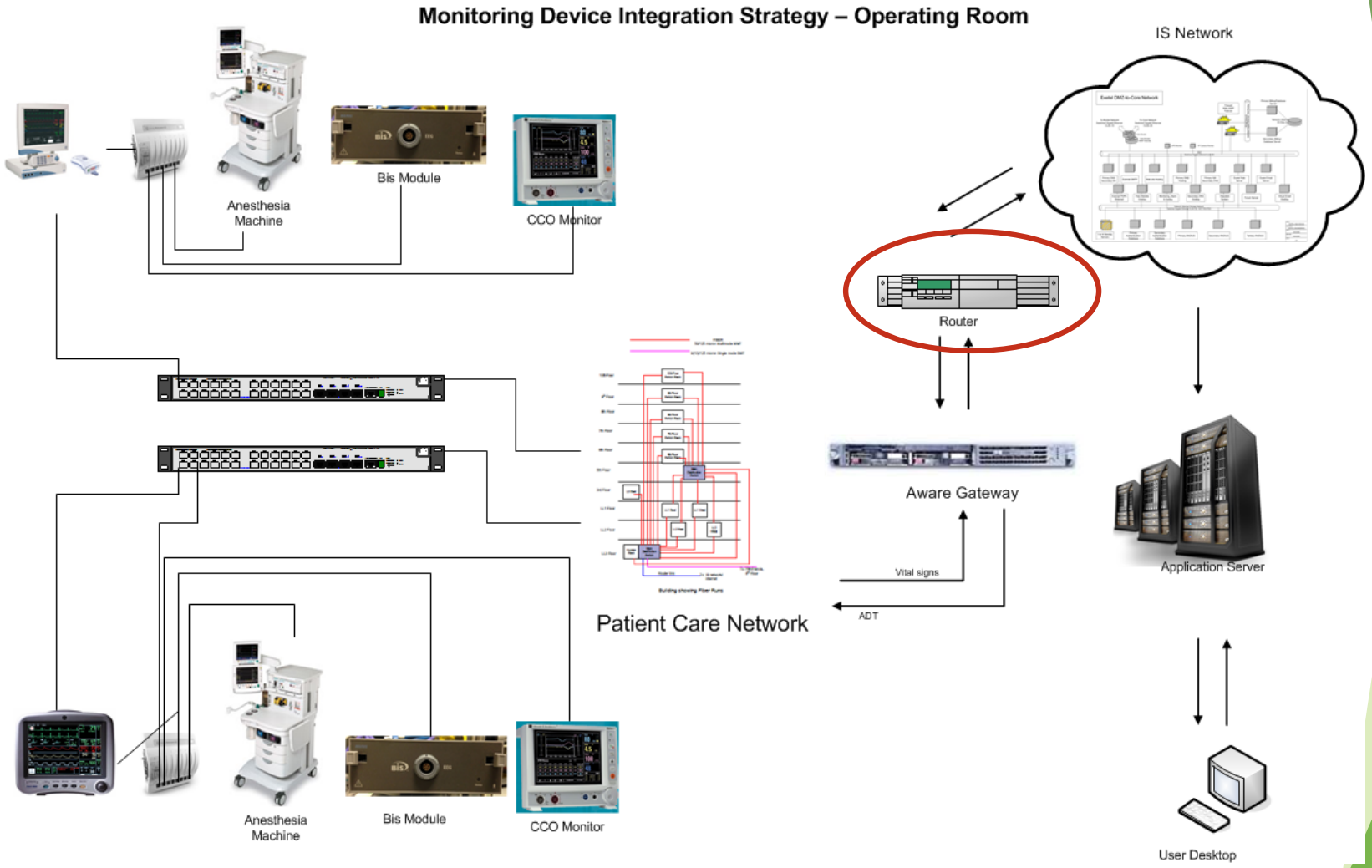
g. Configuration Management

<Describe the organization's configuration management practices for all systems, including whether baseline configuration information is recorded, and the access restrictions implemented to enforce change management. Describe the organization's change management process. >

Directly connected devices on your IS network

- Discuss use of an SMDZ
- Contain devices in a dedicated zone
  - Limit traffic as much as possible within that zone
- Device configuration
  - Open ports configurations are not desired
  - ↓ Risk posture by working with your IS department
- Collaborative & participate in the IS vendor security reviews
- Realize that one device with a weak security profile can expose your entire IS network

Patient Care Networks or Vendor Networks connected to IS



Patient Care Networks or Vendor Network connected to IS

- Examples include:
  - Dedicated real-time patient care networks
  - vendor serial networks connected to IS
- Use of Routers are usually preferred
  - Limit traffic in and out
  - If using HSRP (Hot standby router protocol) Routers ensure that they are configured as well
- Often in an SMDZ with similar devices that may need to interact with each other
- Information security plan reviews for network security of both networks

The Process: Connecting Devices

- Collaborate EARLY with your IS department to start the review process
- Have Security Surveys completed beforehand
- Understand/identify clinical workflow so that the configurations do not compromise clinical care
- Test and validate the system/interface through several scenarios
- Stay current for security level changes in your institution
- Be conscious of software upgrades!
  - Impact on security profile

Lessons learned

- You will have to interface devices to meet the clinical workflows
  - EMRs
  - Communication systems
- It is **not** a static process
- Hold the vendors accountable to meet current security standards
- Minimize customization for ease of support
- Develop training plans
- Verify and test your configurations
- Develop and practice downtime procedures

Contact information

L. Michael Fraai: lfraai@bwh.harvard.edu

BRIGHAM HEALTH
BWH BRIGHAM AND WOMEN'S HOSPITAL

LinkedIn:

https://www.linkedin.com/in/michael-fraai-1b777b3

Bridget Moorman, CCE
BSME, MSBME,
MAS Healthcare Informatics
President
BMoorman Consulting, LLC

Bridget A. Moorman has 28 years' experience in the clinical engineering field and currently consults internationally across the healthcare technology industry specializing in medical device interoperability and integration. She has worked for Kaiser Permanente doing strategic technology management for cardiovascular services, patient monitoring, OB/GYN data management and biomedical device interfacing to the EPIC EMR system. She has also worked for University Medical Center in Tucson, AZ, as a clinical engineer and supporting the artificial heart program. She served as Chair of the CCE Board of Examiners from 2011-2013.

Medical Versus Information Technology

““To protect the network, DoD officials enforce strict cyber standards on all information technology. Medical devices, however, are not "information technology," explained McGraw. Rather, they are "medical technology." It is a subtle yet significant difference.

Information technology includes computers and supporting equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services and related resources.

Medical technologies are single purpose systems intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease.”

Crown, Ellen. “Army Medical Device Cyber Team Balances Benefits and Risks of Technology.” 19 Oct 2018. https://www.army.mil/article/212688/army_medical_device_cyber_team_balances_benefits_and_risks_of_technologyCp

Overview

- Definitions
- Purpose of networking
- Questions to ask
- Flow diagrams for determination
- Exercise
- Keep in mind

Definitions

- Definition of safe
  - secure from liability to harm, injury, danger, or risk
- Definition of networking
  - use of a system of computers and peripherals that are able to communicate with each other
- Definition of medical device
  - any article or healthcare product intended for use in the diagnosis of disease or other conditions, or the use in the care, treatment of prevention of disease which does achieve any of its primary intended purposes by chemical action of by being metabolized (FDA)

Purpose of Networking

- Data flow
  - transmission to another system
- Data aggregation/association/affiliation
  - example: patient demographics associated with physiological measurement
  - centralization of patient information
- Communication with minimal manual or human intervention

Questions to ask

- How is device used/data used in clinical workflow?
- How fast is workflow?
  - Episodic or long-term
  - Real-near-real time
  - Validation
  - Store-forward
- What type of networking?
  - Wired
  - Wireless
  - None
- How is networking capability accomplished on the device?
  - Dongle
  - Embedded

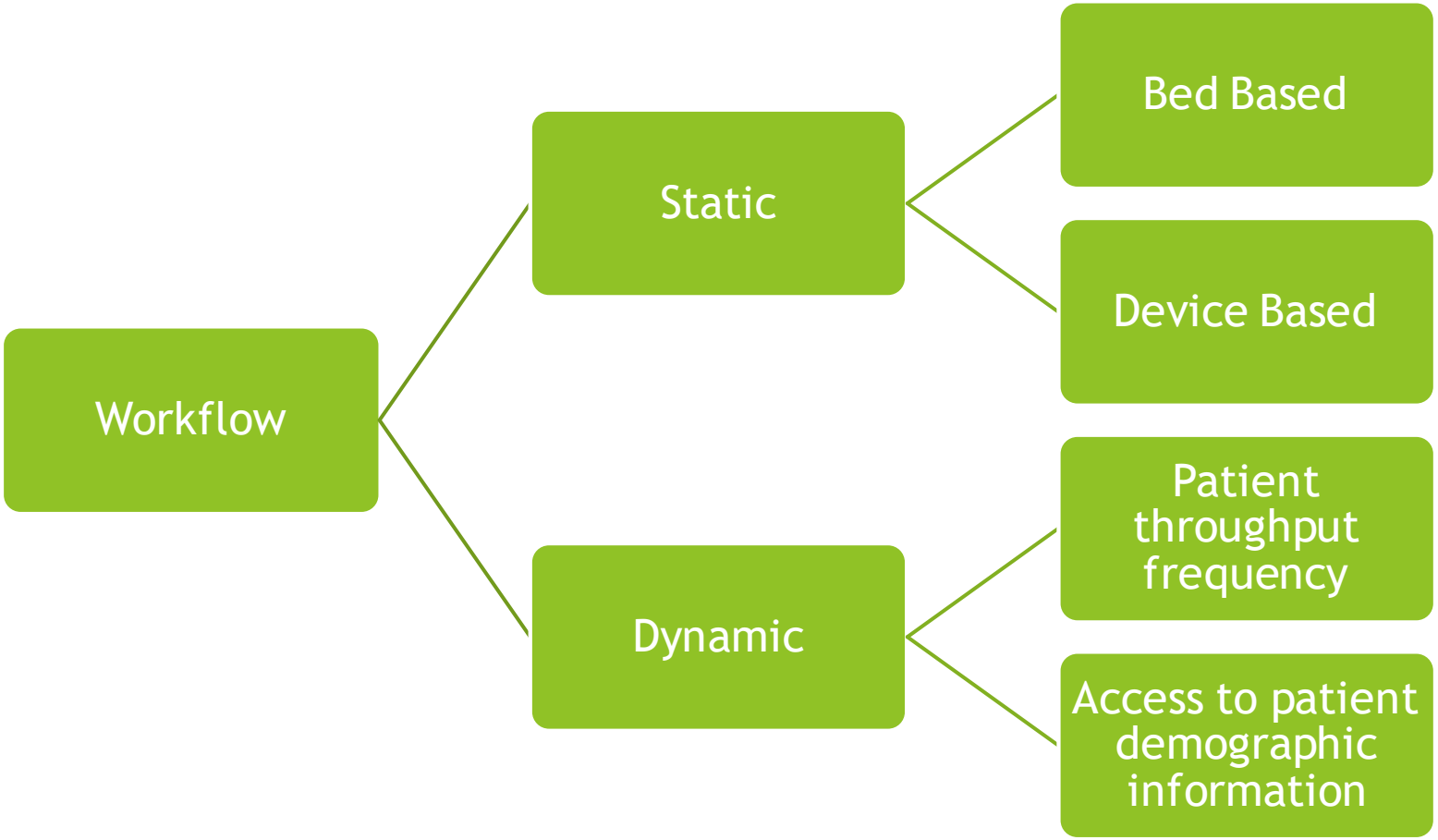
Questions to ask

- What is range of device (use)? Fixed? Mobile?
  - Examples: scale, monitor for ICU/ER
- Is the device part of another system?
  - Monitor to central to gateway
- How sophisticated is the networking protocol on the device?
  - Static or dynamic IP?
- How much bandwidth is required?
  - Example: Telehealth-dermatology needing high fidelity video

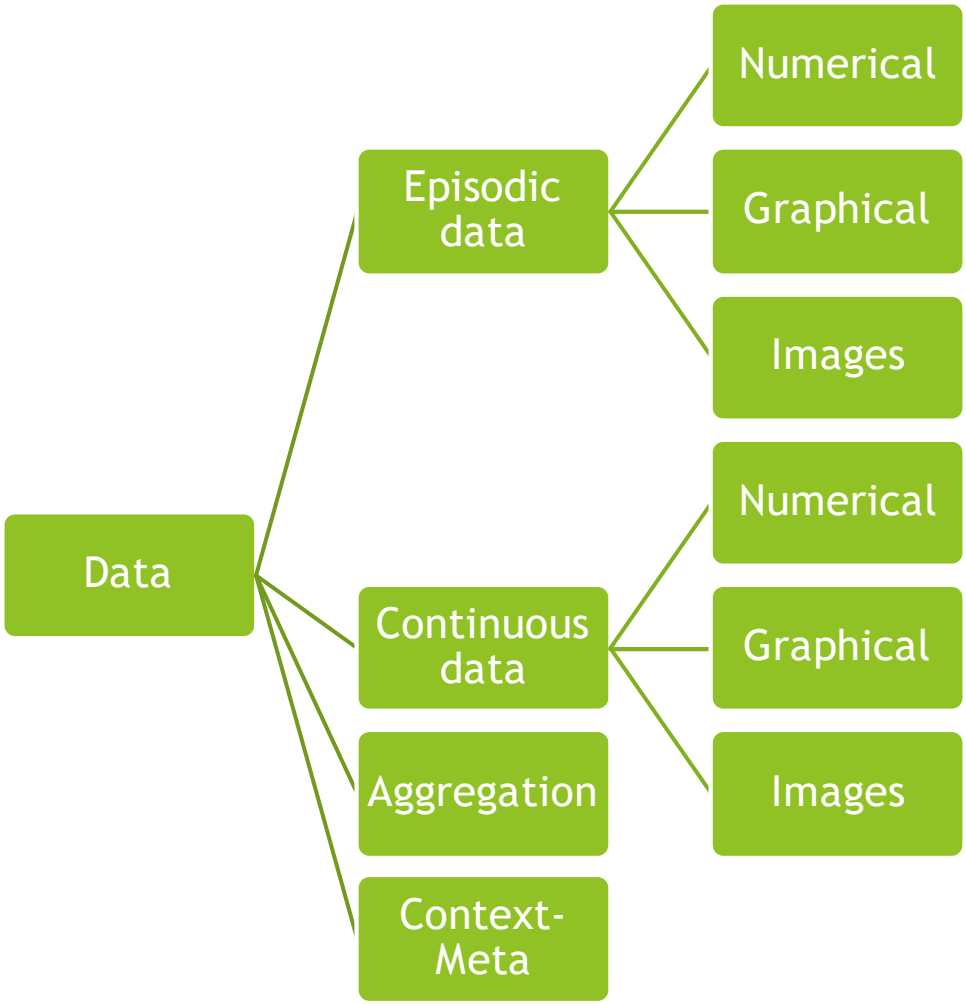
Questions to ask

- Outside Healthcare Enterprise
  - Location determining availability of quality telecommunication capability
    - Ex: Home situation
      - Store and forward?
      - Plain old telephone service (POTS)?

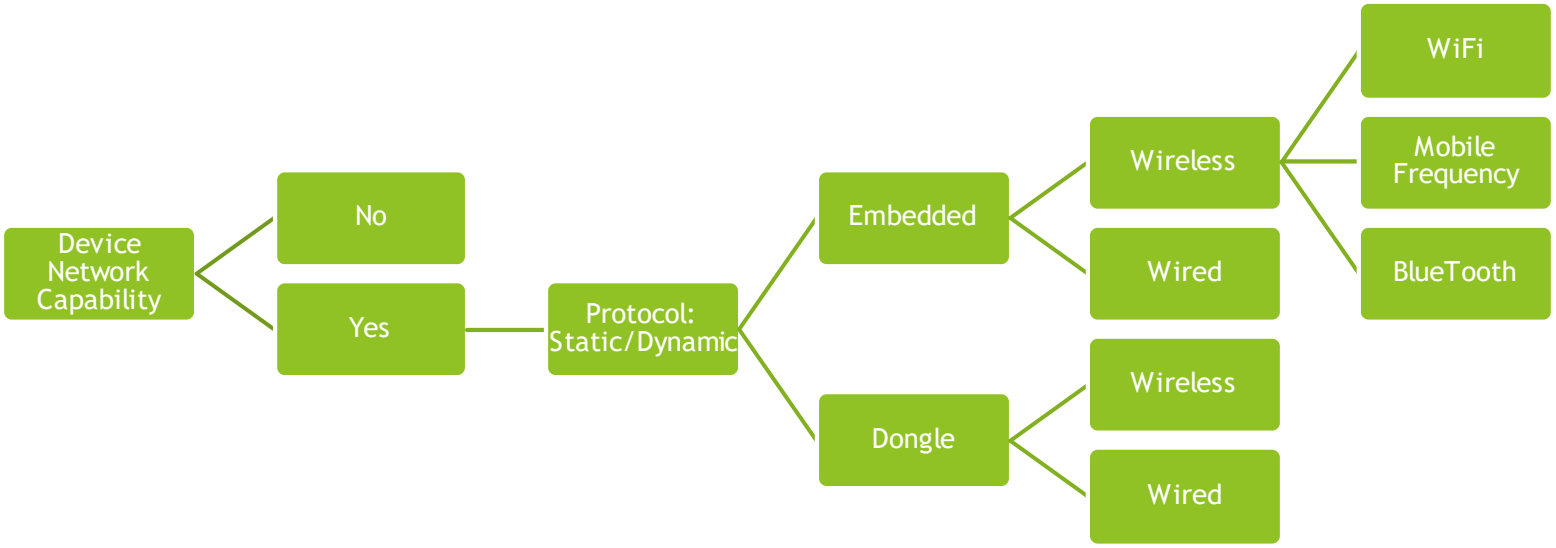
Flow diagrams for determination: Workflow



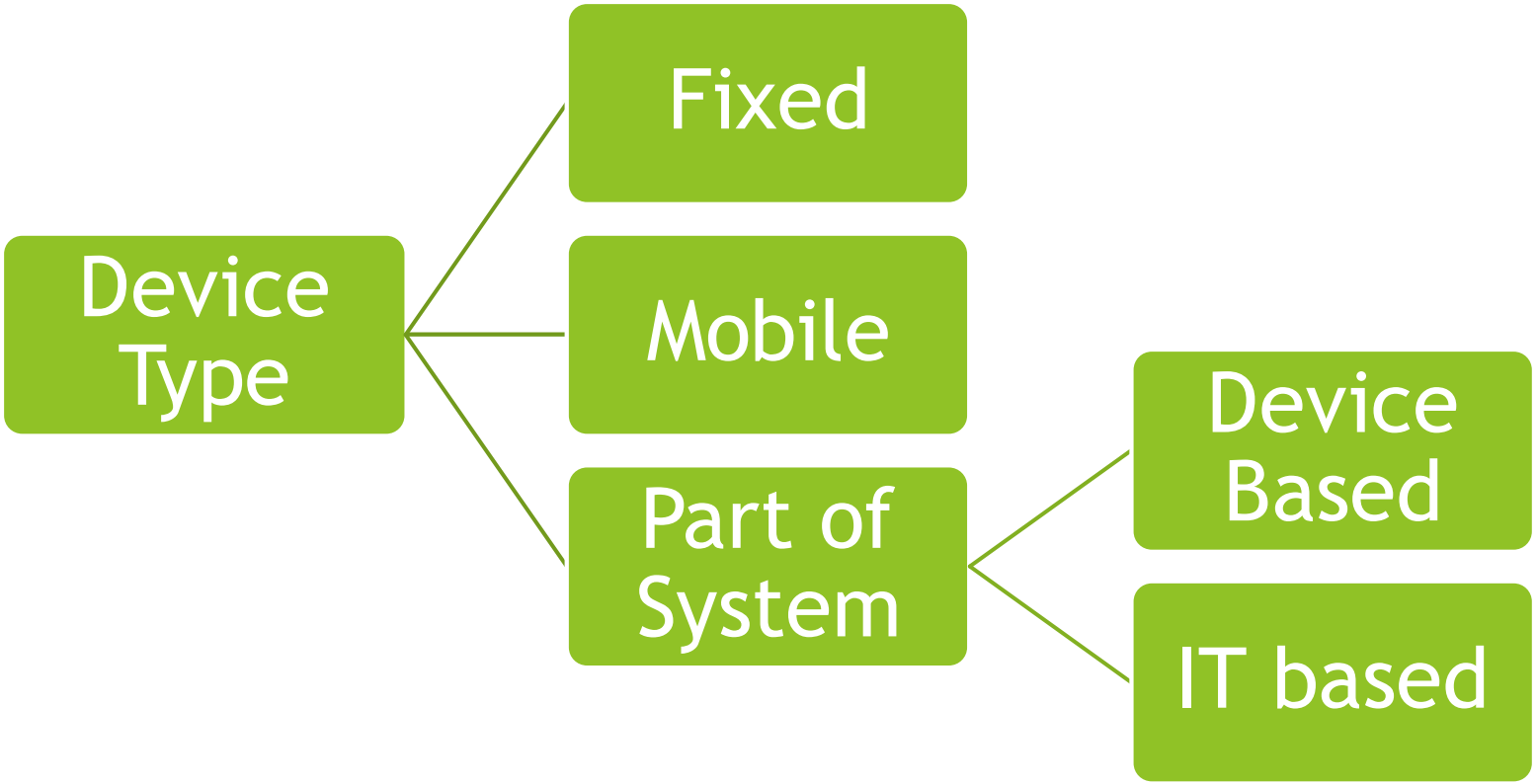
Flow diagrams for determination: Data



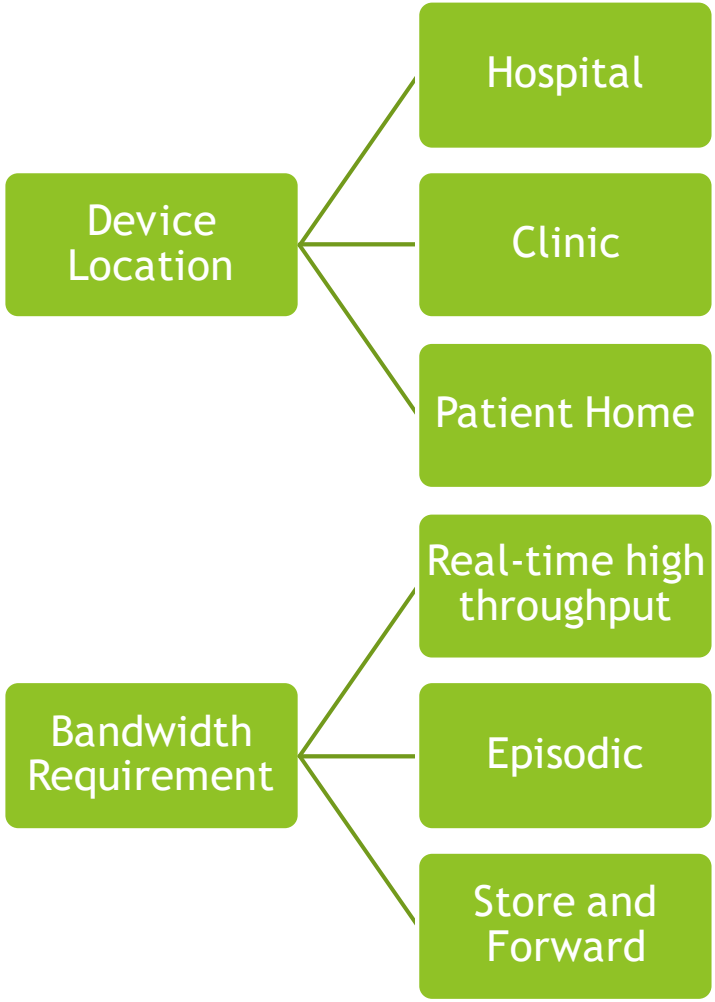
Flow diagrams for determination: Network capability



Flow diagrams for determination: Device type



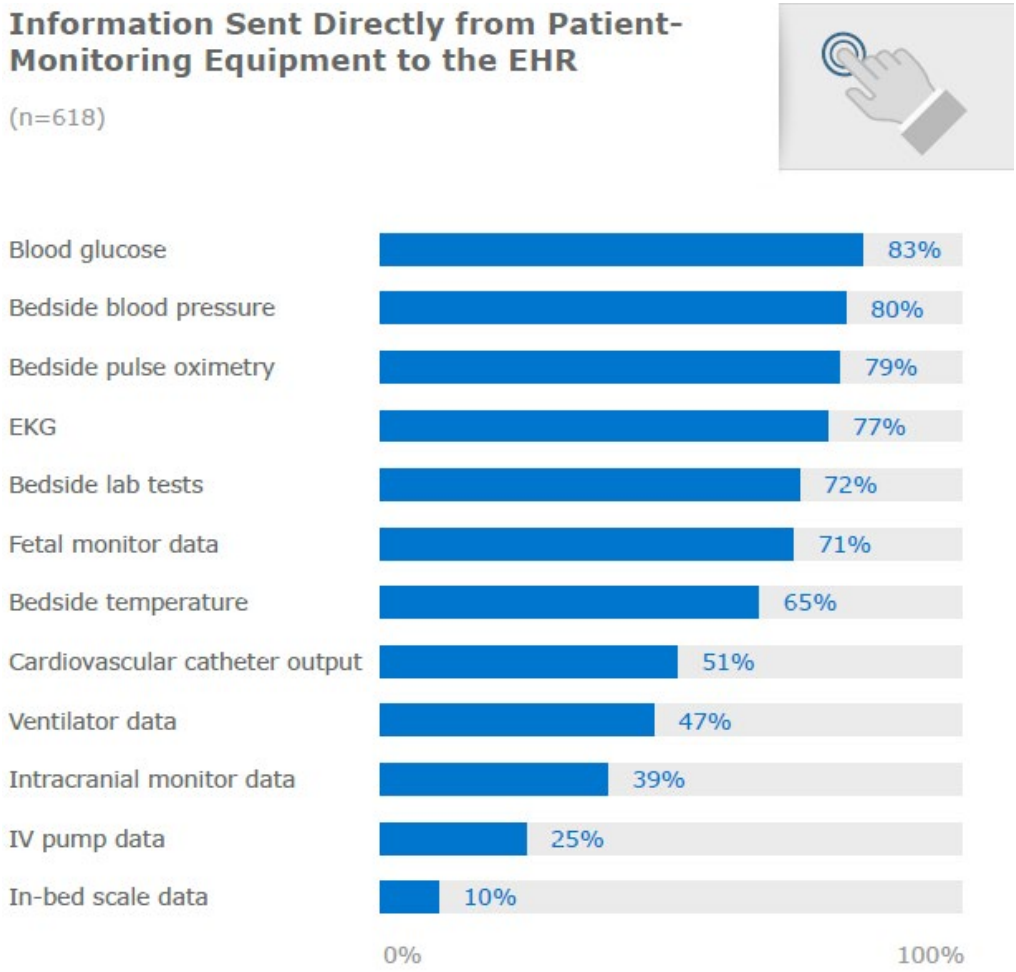
Flow diagrams for determination: Location and bandwidth



Exercise

- Should scales in clinic be connected to network?
- Should monitors in ER be connected to network?
- Should specialty devices in ICU (ECMO monitor) be connected to network?
- Should monitors in ICU be connected to network?

CHIME: Healthcare's most wired results 2018

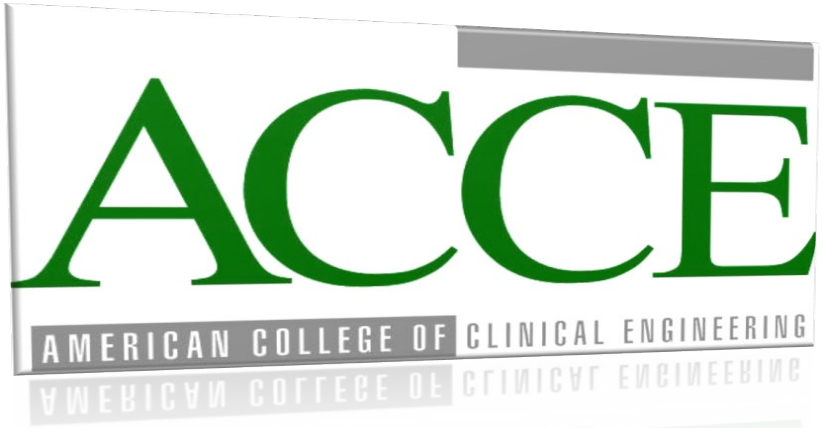


https://chimecentral.org/wp-content/uploads/2018/10/Healthcares-Most-Wired—National-Trends-2018-FINAL.pdf

Keep in mind

- Just because you can connect a medical device to a network does not necessarily mean you should
- Need to understand workflow, the environment and the definition of safe in those situations!

Questions and Discussions



Emerging Technologies and their Impact on the Hospital Operations

Thomas Skorup, MBA, FACHE
Vice President, Applied Solutions
ECRI Institute
tskorup@ecri.org

Session Description

- In this session, participants will learn about emerging technologies that may impact hospital operations and patient outcomes. Mr. Skorup explores the challenges related to successfully forecasting healthcare and technology innovation. Further, he reviews specific leading edge technologies that ECRI Institute and other leading organizations predict will disrupt healthcare delivery in the coming years. Strategies are discussed for addressing challenges related to technology adoption.

About the speaker

Thomas Skorup, MBA, FACHE
Vice President, Applied Solutions
ECRI Institute

- Leads ECRI Institute's Applied Solutions Group onsite consulting service, and manages major projects with healthcare organizations.
- More than 30 years experience forecasting, planning, procuring, and managing the unique challenges that healthcare technology poses to healthcare service delivery.
- Adjunct Faculty, School of Nursing, Villanova University
- Board certified in healthcare management and a Fellow of the American College of Healthcare Executives.
- MBA, Health Administration, Fox School of Business, Temple University
- BS, Biomedical Engineering Technology, Milwaukee School of Engineering

How ECRI Started

- A fiercely independent, nonprofit, mission focused organization committed to improving the **safety, quality, and cost effectiveness** of healthcare through evidence-based research and testing, benchmarking, and collaboration with the healthcare community

"Anger is a great source of energy. I focused it on improving technology and patient safety."

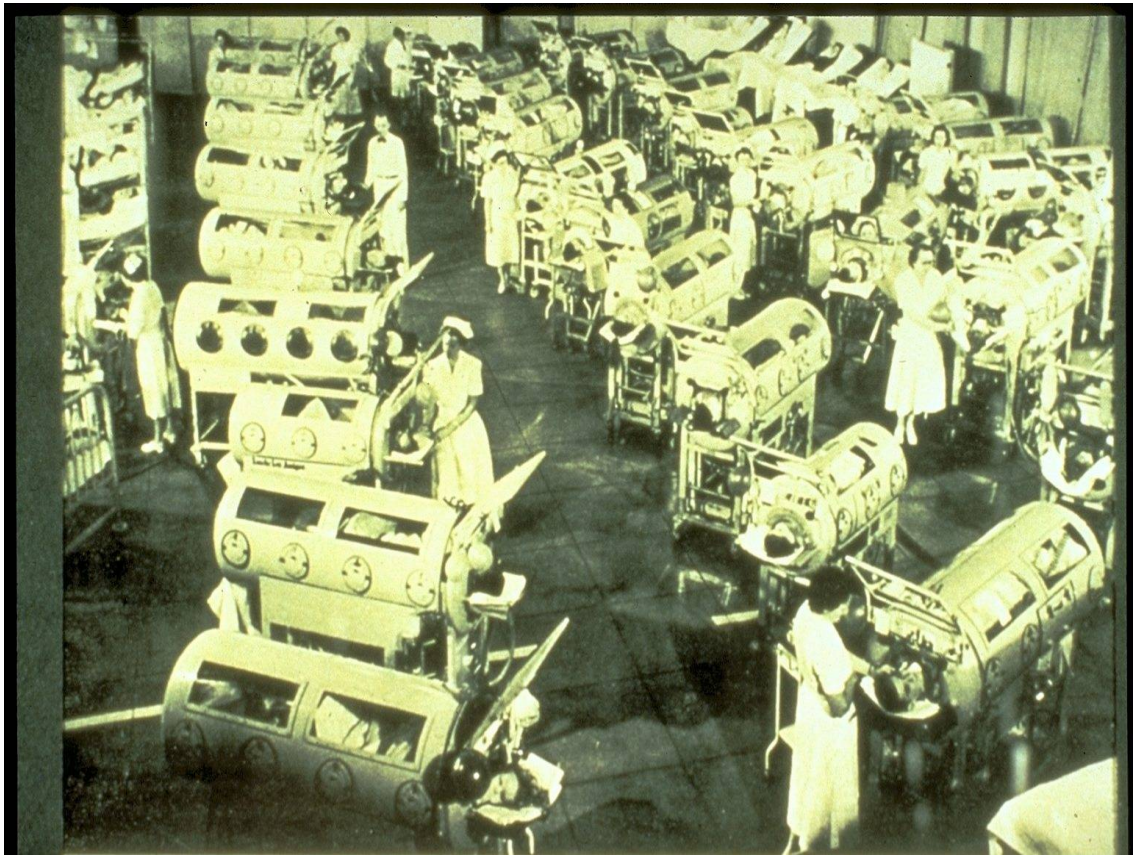
- Joel J. Nobel, MD, Founder of ECRI

Outline

- **Building a Bridge To The Future**
  - The Forecasting Chasm—Seeing around corners
  - The Technology Chasm—Where is technology headed?
- Action Steps
  - Strategies for success
  - Three technology truths

What seems obvious …

… may not be!



Ignore trends at your peril…

Kodak once had 85% of photographic film business!

In the U.S. patients want robotic prostatectomies…

The First Digital Camera (1975)

BY SCOTT BEALE ON AUGUST 20, 2010

Kodak engineer Steve Sasson talks about how he created the first digital camera in December 1975.

Foolish Tech Prediction 1
Thomas Watson, President of IBM,1943

- "I think there is a world market for maybe five computers."

Source PCWorld.com: Strohmeyer, R. (December 31, 2008). The 7 Worst Predictions of All Time. Retrieved from https://www.pcworld.com/article/155984/worst_tech_predictions.html?page=2

Foolish Tech Prediction 2
Darryl Zanuck, Executive at 20th Century Fox, 1946

- Television won't be able to hold on to any market it captures after the first six months. People will soon get tired of staring at a plywood box every night."

Source PCWorld.com: Strohmeyer, R. (December 31, 2008). The 7 Worst Predictions of All Time. Retrieved from https://www.pcworld.com/article/155984/worst_tech_predictions.html?page=2

Foolish Tech Prediction 3
Alex Lewyt, President of Lewyt Vacuum Company, 1955

- "Nuclear-powered vacuum cleaners will probably be a reality within ten years."

Source PCWorld.com: Strohmeyer, R. (December 31, 2008). The 7 Worst Predictions of All Time. Retrieved from https://www.pcworld.com/article/155984/worst_tech_predictions.html?page=2

Foolish Tech Prediction 4
Ken Olsen, Founder of Digital Equipment Corporation, 1977

- There is no reason anyone would want a computer in their home."

Source PCWorld.com: Strohmeyer, R. (December 31, 2008). The 7 Worst Predictions of All Time. Retrieved from https://www.pcworld.com/article/155984/worst_tech_predictions.html?page=2

Foolish Tech Prediction 5
Robert Metcalfe, Founder of 3Com, 1995

- "Almost all of the many predictions now being made about 1996 hinge on the Internet's continuing exponential growth. But I predict the Internet will soon go spectacularly supernova and in 1996 catastrophically collapse."

Source PCWorld.com: Strohmeyer, R. (December 31, 2008). The 7 Worst Predictions of All Time. Retrieved from https://www.pcworld.com/article/155984/worst_tech_predictions.html?page=2

A few common technology themes…

- Look for the “breakthroughs”, but also the “bridges”
- Get Real---Become a “Technology Realist”

(Neither a Luddite nor a technophile be)

- Understand the evidence.

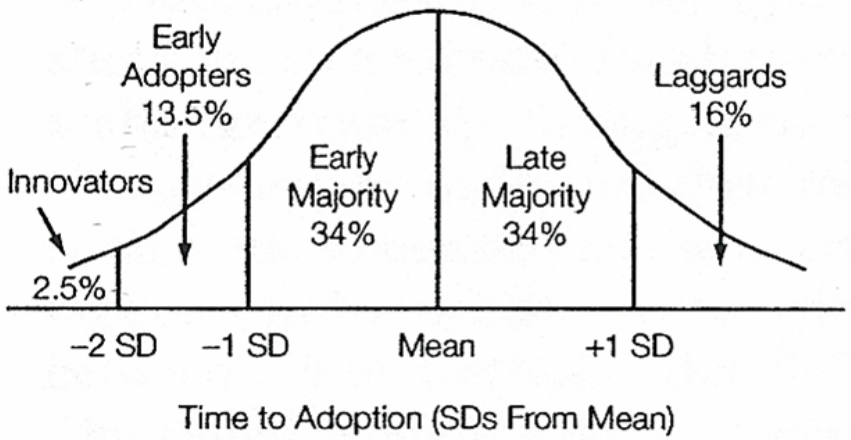
The Forecasting Chasm

- Trends are easier to predict than breakthroughs and are often evolutionary in nature.
  - **Evolutionary or Revolutionary?**
    - Laparoscopic Cholecystectomy
    - 3D Laparoscopic Imaging?
    - Drug-eluting stent?
    - Robotically-assisted laparoscopic surgery?
    - Transcatheter aortic valve replacement?

To thy own self be true…

where are you?

Figure 2. Adopter Categorization on the Basis of Innovativeness



Reprinted with permission from Rogers.[21]

D. Berwick,JAMA, April 16, 2003-Vol. 289, No. 15 (Reprinted)

Does this new technology provide a clinical or strategic advantage?

The Forecasting Chasm

- Watch for the tipping point – Malcolm Gladwell.
  - Law of the Few – Connectors
  - The Stickiness Factor
  - The Power of Context

  - BRCA1/2 mutation testing
  - Others?

Which new technology will stick?

And actually make a difference?

And what are outcomes we expect from technology in healthcare?

- Longer life?
- Better life?
- Higher productivity?
- Healthier populations?
- Happier people?

Where is technology headed?

ECRI Institute Top 10 C-suite Watch List

- **ECRI experts polled for topics regarding….**
  - Something newsworthy
  - The potential to positively impact patient outcomes in major illnesses, diseases, or injuries
  - Ready or near ready for implementation
  - Turf wars or, conversely, improved collaboration
  - Improving patient and staff safety
  - A marketplace differentiator

ECRI Institute
Top 10 Hospital C-suite Watch List (2018)

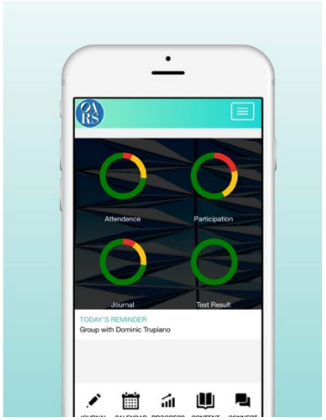
1. Apps for Addiction
2. Direct to Consumer Genetic Testing
3. Acuity-adaptable Rooms
4. Insertable Cardiac Monitor
5. Virtual Reality for Pediatrics
6. Non-medication Treatments for Alzheimer's Disease
7. (Nearly) Pain-free Blood Draw
8. Neonatal MRI System
9. GammaTile™ Cesium 131 vs. Brain Tumors
10. Microhospitals

1. Apps for Addiction

- First prescription digital therapeutic (reSET-O™, PearTherapeutics) to receive FDA clearance app as a prescription-only adjunct treatment

- Nearly doubled the rate of abstinence and increased retention in treatment

- Benefits include:
  - Fewer patient relapses
  - Decreases in patient admissions or readmissions
  - Reduction in overdose incidents and ED visits

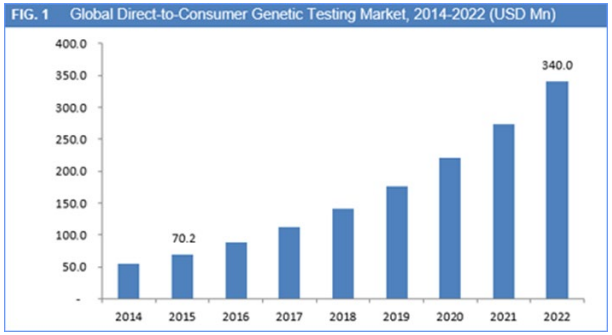


2. Direct-to-Consumer (DTC) Genetic Testing

- **Emerging Uses (beyond ancestry):**
  - Epigenetic analysis to determine biological age (as compared to chronological age)
  - Diet & exercise strategies based on individual genotype
  - Customized advice on skin care (topical creams, professional treatments)

- Growing implications for hospitals and health systems.

- Increased healthcare service demands from patient anxiety from unexpected test results.



Source: Credence Research

3. Acuity-adaptable Rooms

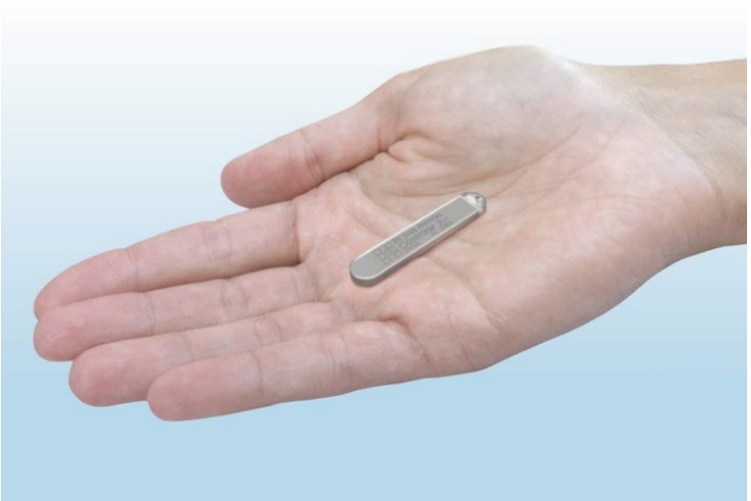
- Keeps a patient in the same room from admission to discharge, regardless of acuity level. Patient transfers/handoffs are a known safety issue.

- **Benefits:** improve workflows and patient safety, decrease LOS, reduce costs.

- **Challenges:**
  - Maintaining staff competencies across all acuity levels
  - Choosing right patient groups: cardiac, transplant, oncology
  - Accommodating care standards for each acuity level (e.g., sightlines for critical care vs. privacy for improved patient)

4. Insertable Cardiac Monitor

- 6 million people in the U.S. have atrial fibrillation (AF).
- Abbott Confirm Rx™ ICM
  - Insertable cardiac monitor transmits to patient's smartphone which sends data to the treating physician
  - Replaces bulky and retrospective Holter recording
  - Provide event marking capability
- Worldwide ICM estimated market at $800M



5. Virtual Reality for Pediatrics

- VR distraction for kids with chronic conditions requiring frequent procedures like infusion therapy or needlesticks.
- Studies have shown a decline in pain for the children and a decline in anxiety scores of their parents.
- appliedVR offers headsets with about 20 different VR experiences
  - At about $2,500-$3,800, plus annual licensing
- Lucille Packard Children's is using VR in all of its patient rooms.

6. Non-medication Treatment for Alzheimer's Disease

- 5.5M Americans have Alzheimer's dementia, which is the 6th leading cause of death in the U.S.
- Transcranial magnetic stimulation (TMS) with computer-based cognitive training (NeuroAD Therapy System) AND the patient's pharmacologic therapy.
  - Full 6-week course costs up to $10,000.
- Received CE mark; denovo FDA clearance pending.

7. Nearly Pain-free Blood Draw

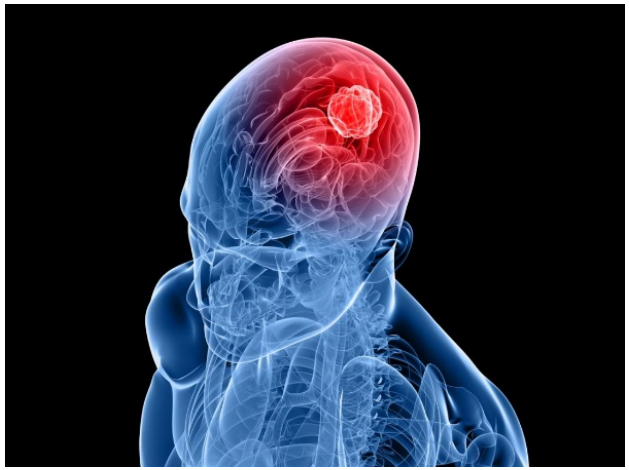
- Reducing blood draw amounts and simplifying blood draws.
- Seventh Sense Biosystems TAP® (touch activated phlebotomy) uses 30 microneedles to collect 100 microliters of blood over 2-3 minutes.
- Targeted audience:
  - Pediatrics who require frequent blood draws
  - Monitoring of outpatient adherence
  - Currently only cleared for A1c testing
- Gates Foundation grant, and LabCorp and Novartis partnerships may accelerate development.

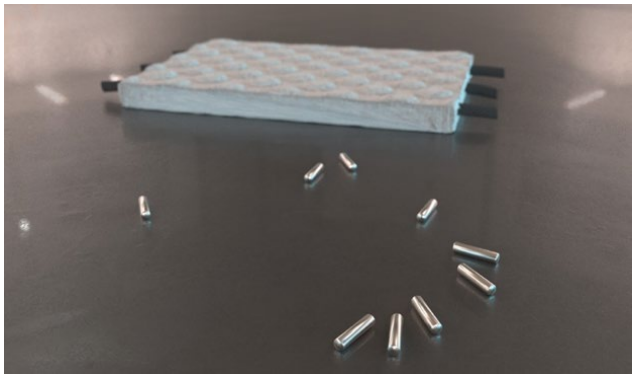
8. Neonatal MRI System

- Reduces risk of neonate transport for MRI for edema or hemorrhage.
- Embrace® Neonatal MR System (Aspect Imaging) is a point-of-care NICU-based MR for <9.9 lbs. neonates.
- Benefits:
  - Integrated incubator to control body temperature and measure vital signs during procedure
  - No safety zone/shielded room
  - Low noise scans

9. GammaTile™ Cesium-131 vs. Brain Tumors

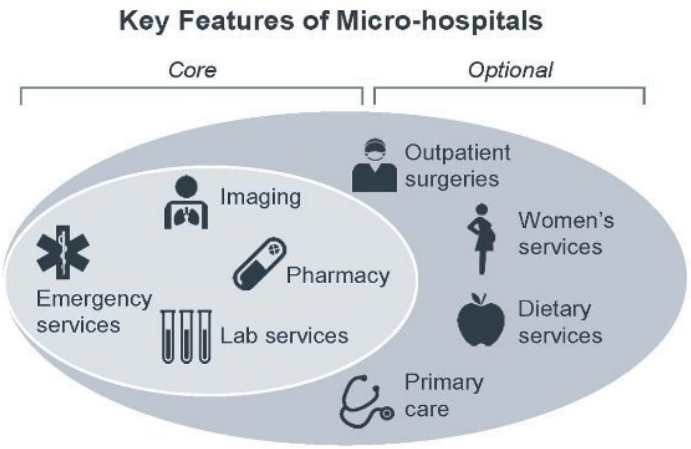
- Reduces time between surgery and radiation treatment.
- Gamma Tile Radiation Therapy System (GT Medical Technologies)
  - Intraoperatively delivered brachytherapy that standardizes seed placement and improves dose targeting
- Cesium-131 seeds incorporated into a bioabsorbable collagen mesh that neurosurgeon and radiation oncologist suture into place.
- Improved survival (4 mos.) and lower cost ($25k) compared to stereotactic radiosurgery
- FDA 510(k) pending





10. Microhospitals

- New less acute care paradigm
- Between an urgent care center and a full service hospital
  - ED and inpatient beds
  - No critical care beds
  - Surgery, pharmacy, radiology
  - Dietary, EVS, Materials
- Branding opportunities in fast growing or underserved areas.
- Beware of cannibalizing existing services that may already be underutilized.



https://pbs.twimg.com/media/Cmnk0IDWEAEcOwl.jpg

Cleveland Clinic
Top 10 Medical Innovations for 2019

#1 Alternative Therapy for Pain: Fighting the Opioid Crisis

#2 The Advent of AI in Healthcare

#3 Expanded Window for Acute Stroke Intervention

#4 Advances in Immunotherapy for Cancer Treatment

#5 Patient-Specific Products Achieved with 3D Printing

#6 Virtual and Mixed Reality for Medical Education

#7 Visor for Prehospital Stroke Diagnosis

#8 Innovation in Robotic Surgery

#9 Mitral and Tricuspid Valve Percutaneous Replacement

#10 RNA-Based Therapies

https://innovations.clevelandclinic.org/Summit/Top-10-Medical-Innovations.aspx

Outline

- Building a Bridge To The Future
  - The Forecasting Chasm—Seeing around corners
  - The Technology Chasm—Where is technology headed?
- **Action Steps**
  - Strategies for success
  - Three technology truths

Strategies for Success

- Implement evidence-based technology decision-making process
- Add organized technology horizon-scanning into your five-year strategic capital plan
- Ensure your healthcare strategy includes a clinical technology strategy

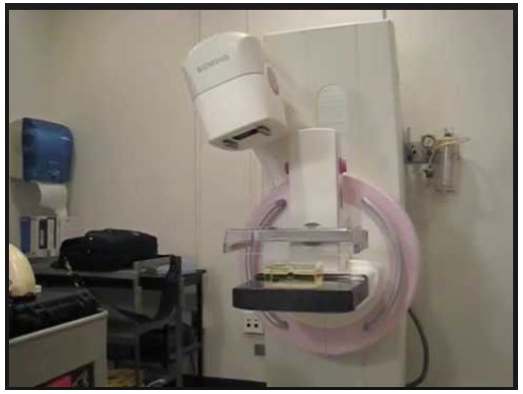
Strategies for Reducing Costs

- Look for collaboration partners
- Look for “standardization” opportunities and “risk mitigation” strategies
- Approach multi-year vendor partnerships carefully

Three Technology Truths

1. Fortune favors the bold (Latin proverb)
2. Facts are stubborn things (John Adams)
3. Data is not the plural of anecdote (various authors)

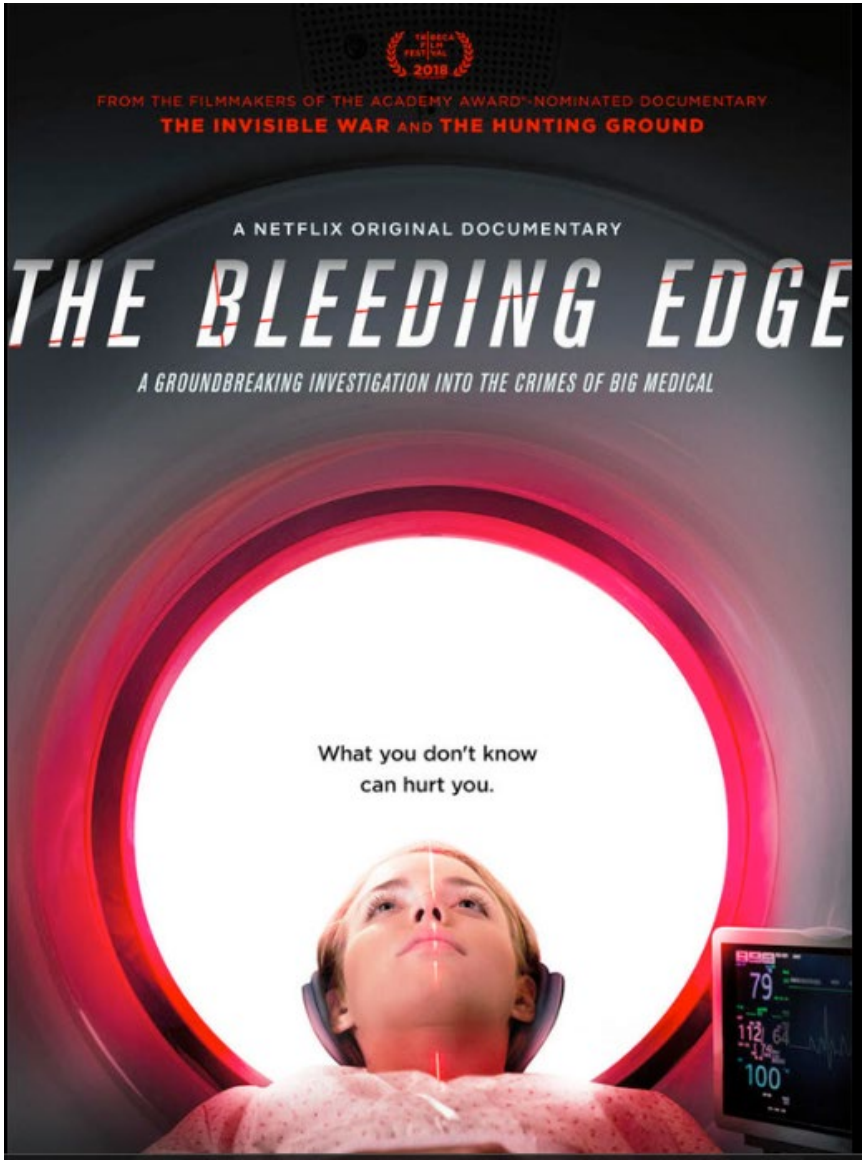
Fortune favors the bold



Facts are stubborn things

Who remembers the Monty Hall problem?

Data is not the plural of anecdote


TRIBECA FILM FESTIVAL 2018
FROM THE FILMMAKERS OF THE ACADEMY AWARD®-NOMINATED DOCUMENTARY
THE INVISIBLE WAR AND THE HUNTING GROUND
A NETFLIX ORIGINAL DOCUMENTARY
THE BLEEDING EDGE
A GROUNDBREAKING INVESTIGATION INTO THE CRIMES OF BIG MEDICAL
What you don't know
can hurt you.

Foolish Tech Prediction 6

Nathan Myhrvold, former Microsoft CTO, 1997

- "Apple is already dead."

Source PCWorld.com: Strohmeyer, R. (December 31, 2008). The 7 Worst Predictions of All Time. Retrieved from https://www.pcworld.com/article/155984/worst_tech_predictions.html?page=2

Questions and Discussions

Long Term Capital Planning

Carol Davis-Smith, CCE
President
Carol-Davis Smith & Associates
Carol@CDSAssoc.com

Jennifer Ott, CCE, FACCE
Medical Equipment Specialist – Project Manager
NorthStar Management, LLC
Jennifer.Ott2@mercy.net

Session Description

- A ***panel discussion*** that will explore diverse perspectives and challenges impacting our ability to define long-term capital plans for medical devices and systems.

- Particular attention will be paid to the impact of networked medical device systems and the inherent challenges of cybersecurity.

- The ***objective*** is to inform clinical engineering and information technology professionals such that they can engage in the capital planning process more confidently and effectively.

Panelists

Carol is a certified clinical engineer with 30 years of experience in academic and not-for-profit medical centers, group purchasing, consulting, and executive leadership. Through collaborative leadership and technical engagement, she has built successful teams across all aspects of the medical device lifecycle.

Carol Davis-Smith, CCE
President / Owner
Carol Davis-Smith & Associates, LLC

Jennifer is a certified clinical engineer with 28 years of experience in academic, for-profit, and not-for-profit healthcare systems. Her current role manages hospital construction projects with a focus on medical equipment planning and implementation. She provides leadership skills to the variety of disciplines necessary for a successful team and project.

Jennifer Ott, CCE, FACCE
Medical Equipment Specialist ~ Project Manager
Northstar Management, LLC

Panelists

Mary is a Registered Nurse with 37 years' experience in the acute and ambulatory settings working mainly with Pediatric patients. She has been a Clinical Manager of the Acute Infusion team with Smiths Medical for 10 years. Her primary focus is collaborating with the acute care customer's multi-disciplinary team from the pre-sale/pre-planning phase through successful implementation of infusion pumps.

Mary Johnson, BSN, RN
Clinical Manager, Acute Infusion - Professional Services
Smiths Medical

Mike is a certified materials & resource professional with 30 years of healthcare experience in children's hospitals and the Association for Health Care Resource & Materials Management (AHRMM). As a supply chain and UDI subject matter expert, he collaborates with health systems, manufacturers, and other industry and regulatory leaders from across healthcare on the advocacy, adoption, and implementation of the UDI.

Mike Schiller, CMRP
Vice President of Healthcare Engagement
Matrix IT

Topics of Discussion

- "Long-term" versus "Short-term" capital planning

- Decision-makers
- Relevant information
- "Approval" versus "Funding"

- Policy – Process – Procedures ("How to")
- Resources – tools, expertise, timing

- Large projects – construction/renovation
- Networked medical devices
- Cyber threats and security

- "Train wrecks" and memorable successes

- CE/IT professionals involvement

The following 3 pages are examples/tools provided by our colleagues at AHRMM

Example Criteria to Rate Equipment

Criteria	High (9)	Medium (3)	Low (1)	Weight
Lifecycle Stage	Exceeding useful life (10 yrs. or greater)	Within normal useful life (between 3 and 9 years)	New technology (0-2yrs old)	25%
Service History	CES overall rating Poor based on # of service events and CAR (service Cost to Asset Ratio)	CES overall rating Fair based on # of service events and CAR (Cost to Asset Ratio)	CES overall rating Good or Excellent based on # of service events and CAR (Cost to Asset Ratio)	30%
Utilization	Top 25% of usage within Allina	Usage between 25% and 75% of usage within Allina.	Lowest 25% of usage within Allina	15%
End of Service Life, Parts Availability	EOL and/or CES can not support	OEM has not declared EOL but useful life has been exceeded	OEM has not declared EOL, parts are readily available	30%

AHRMM_CT_Initial_2018

Device Category	Manufacturer	Model	Description	Facility	Department Name	ECN	In Svc Year	EOL/EOS Score	CES rating
CT Scanner						3408985	2006	3	Poor
CT Scanner						3206119	2006		
CT Scanner						3104571	2003	3	Fair
CT Scanner						6205707	2006	3	Fair
CT Scanner						6207225	2007	3	Fair
CT Scanner						3203851	2007	3	Good
CT Scanner						3412901	2006	3	Good
CT Scanner						4000327	2005	3	Good
CT Scanner						3115144	2007	3	Excellent
CT Scanner						3203102	2014	1	Fair
CT Scanner						3118581	2013	1	Excellent
CT Scanner						3118583	2011	1	Good
CT Scanner						3118582	2012	1	Good
CT Scanner						3500721	2010	1	Good
CT Scanner						4601871	2008	1	Good
CT Scanner						4604403	2014	1	Good
CT Scanner						4700539	2012	1	Excellent
CT Scanner						3116672	2009	1	Good
CT Scanner						4603308	2011	1	Excellent
CT Scanner						3414981	2013	1	Excellent
CT Scanner						3127989	2016	1	Excellent
CT Scanner						3505492	2015	1	Good
CT Scanner						4011459	2016	1	Excellent
CT Scanner						4104255	2017	1	Excellent
CT Scanner						3417941	2015	1	Excellent
CT Scanner						3405368	2016	1	Excellent
CT Scanner						2402141	2017	1	Excellent
CT Scanner						3128748	2016	1	Excellent
CT Scanner						4300100	2016	1	Excellent
CT Scanner						4501374	2016	1	Excellent
CT Scanner						6303588	2016	1	Excellent
CT Scanner						3111276	2013	1	Excellent
CT Scanner						4401111	2009	1	Good

AHRMM_CT_Assessment_Scored_2018

Device Category	Manufacturer	Model	Description	Facility	Department Name	ECN	In Svc Year	Lifecycle Score	End of Support Rating	EOL/EOS Score	CES rating	CES Score	Current Annual Volumes	Utilization Score	TOTAL SCORE
CT Scanner						3408985	2006	9		3	Poor	9	22,166	8	74
CT Scanner						3104571	2003	9		3	Fair	3	3,271	2	47
CT Scanner						6205707	2006	9		3	Fair	3	2,868	1	45
CT Scanner						6207225	2007	9		3	Fair	3	1,166	1	45
CT Scanner						3203851	2007	9		3	Good	1	4,632	2	41
CT Scanner						3412901	2006	9		3	Good	1	3,694	2	41
CT Scanner						4000327	2005	9		3	Good	1	796	1	39
CT Scanner						3115144	2007	9		3	Excellent	1	586	1	39
CT Scanner						3203102	2014	3		1	Fair	3	26,247	9	34
CT Scanner						3118581	2013	3		1	Excellent	1	14,519	6	24
CT Scanner						3118583	2011	3		1	Good	1	14,519	6	24
CT Scanner						3118582	2012	3		1	Good	1	14,519	6	24
CT Scanner						3500721	2010	3		1	Good	1	7,710	3	19
CT Scanner						4601871	2008	3		1	Good	1	6,126	3	19
CT Scanner						4604403	2014	3		1	Good	1	6,126	3	19
CT Scanner						4700539	2012	3		1	Excellent	1	5,723	3	19
CT Scanner						3116672	2009	3		1	Good	1	770	1	16
CT Scanner						4603308	2011	3		1	Excellent	1	207	1	16
CT Scanner						3414981	2013	3		1	Excellent	1	30		15
CT Scanner						3127989	2016	1		1	Excellent	1	8,050	3	13
CT Scanner						3505492	2015	1		1	Good	1	7,711	3	13
CT Scanner						4011459	2016	1		1	Excellent	1	7,196	3	13
CT Scanner						4104255	2017	1		1	Excellent	1	7,142	3	13
CT Scanner						3417941	2015	1		1	Excellent	1	6,870	3	13
CT Scanner						3405368	2016	1		1	Excellent	1	6,670	3	13
CT Scanner						2402141	2017	1		1	Excellent	1	5,091	2	12
CT Scanner						3128748	2016	1		1	Excellent	1	4,930	2	12
CT Scanner						4300100	2016	1		1	Excellent	1	4,761	2	12
CT Scanner						4501374	2016	1		1	Excellent	1	4,076	2	12
CT Scanner						6303588	2016	1		1	Excellent	1	2,949	1	10
CT Scanner						3111276	2013	3		1	Excellent	1			15
CT Scanner						4401111	2009	3		1	Good	1			15

PANEL DISCUSSION

Note: Presentation slides will be posted on ACCE website
www.accenet.org

Thank you for attending!

HIMSS and ACCE have compiled the following sessions, as a recommendation, which may be of interest to you. All times listed are ET.

Health Technology Alliance & ACCE Awards Reception
Tuesday, February 12 | 6:00 pm– 8:00 pm | Convention Center | Level 2 W240C

Network with ACCE members, experts from Clinical Engineering, Health Technology Management, and Medical Device Domain - all are welcome to attend! Join Arif Subhan, President/ACCE and Steven Wretling, CTIO/HIMSS in congratulating the 2019 ACCE/HIMSS Excellence in Clinical Engineering and Information Technology Synergies Award recipient. Scan QR code to RSVP

CIO Perspective - Strong IT requires a Mighty IT/HTM Bond
Wednesday, February 13 | 9:00am – 9:45am
Convention Center | HIMSS Spot | Lobby C

Investments in clinical technologies are increasingly becoming integrated into healthcare organizations' IT infrastructure. The bond between IT and HTM must be strong and cohesive to ensure a strong infrastructure that fully supports care delivery. This session describes success factors in this relationship and highlights one organization's journey. Presenters Pam Arora, SVP and CIO at Children's Health, and Sue Schade, Principal at StarBridge Advisors. Both AAMI board members and previous recipients of the CHIME-HIMSS John E. Gall Jr. CIO of the Year Award.

Presenting the Case of Cybersecurity Education of Clinicians – ACCE collaborator sponsored session
Wednesday, February 13, 2019. 1:00 – 2pm | Convention Center | Level 3 W311A

Today's security risks are too complex and the risk to care delivery and patient safety is too high for cybersecurity to be relegated to the purely technical realm. Cybersecurity programs can only succeed if based on a holistic approach that involves a constructive partnership between stakeholders. This session will explore how organizations can improve cybersecurity when decisions are made as a partnership between security-educated clinicians and security professionals that balances patient and societal needs for health, safety AND security. Presenters: Axel Wirth, Distinguished Technical Architect, Symantec Corporation and Dr. Joseph Schneider, Clinical Assistant Professor, UT Southwestern Medical Center.

A Practical Approach to Medical Technology Capital Planning
Thursday, February 14, 2019; 11:30am-12:30pm | Convention Center | Level 3 | W315A

Most healthcare organizations usually have a set capital budget for medical technology acquisitions. In this day and age, technology has become increasingly complex, devices are interfacing with each other as well as Electronic Medical Records; and CyberSecurity has taken a front and center seat on medical equipment and systems decisions. In this session, we will explore how three different leading healthcare organizations have coped with these issues, different strategies used to address them, and lessons learned during this process. Speakers: Ilir Kullolli, Director, Clinical Technology and Biomedical Engineering, Stanford Children's Health and Kevin Kreitzman, Assistant. Director, Clinical Engineering, Brigham and Women's Hospital.

Join the Health Technology Alliance http://www.healthtechnologyalliance.org/ or scan QR:

Sponsored by

ACCE AAMI HIMSS

for more networking and educational opportunities.

Health Technology ALLIANCE | Advancing the Safety and Security of Devices and Systems