

# 2026 ACCE CE-IT Symposium

26

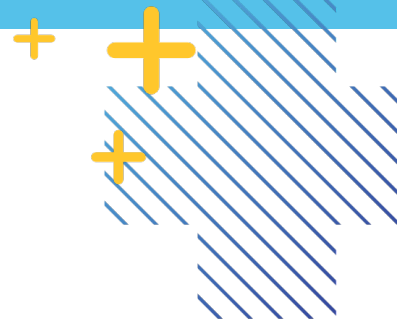
# Future-Ready Healthcare: From Evolution to Revolution

March 09, 2026; 8:30am – 4:00pm

# Meet Our Coffee Break Sponsor



# Meet Our Speakers



**Perry Kirwan**  
Executive, Clinical Engineering  
Sutter Health



**Samantha Jacques**  
VP Clinical Engineering  
McLaren Health



**Mahesh Chintakunta**  
Sr Director, Cybersecurity Ops  
RUSH



**Bill Riley**  
Sr Information Security Engineer  
Mayo Clinic



**Ernest Liu**  
Sr. Engineer  
Siemens

# Today's Program



8:30AM	<b>Opening</b>		
8:40AM - 9:40AM	<b>How Public/Private Partnerships can help you! – learn about the Health Sector Coordinating Council</b>	From obtaining free guidance on cutting edge issues to learning about how other organizations tackle challenges – come learn about what the Health Sector Coordinating Council Cybersecurity Working Group has to offer. Learn about our initiatives, best practice guidance, how we work to inform our government partners, and what we can do for you.	Samantha Jacques, Vice President of Clinical Engineering at McLaren Health
9:40AM - 10:30AM	<b>Uncovering 'Invisible' Medical Devices: How a cyber ecosystem can help</b>	An ecosystem of cybersecurity tools helped improve the visibility of a hospital system's connected medical devices by 60%. This is achieved by integrating cybersecurity tools with a medical device security management platform (MDSM) over a few quarters. This largely helped to understand the risks associated with the hospital and provided an opportunity to address them.	Mahesh Chintakunta, Sr. Director Cybersecurity Ops, RUSH
10:30AM - 10:45AM	<b>BREAK</b>		
10:45AM - 11:30AM	<b>Advancing Secure, IT-Ready Medical Devices: A Mayo Clinic &amp; Siemens Collaboration</b>	Healthcare Delivery Organizations (HDOs) increasingly need medical devices that integrate seamlessly with modern cybersecurity and network management tools. Mayo Clinic's HTM program has been advocating for this shift, pressing manufacturers to design equipment that functions more like contemporary IT assets. Many manufacturers have expressed concerns about feasibility, risk, and regulatory complexity—but Siemens has become the first to break new ground.  In this session, Siemens will demonstrate a next-generation ultrasound platform engineered to operate within standard IT frameworks, enabling native compatibility with enterprise cybersecurity controls, patching workflows, and endpoint management tools. Mayo Clinic will share how both organizations collaborated to test, validate, and prove these capabilities in real clinical and technical environments.	Bill Riley, Sr Security Engineer, Mayo Clinic  Ernest Liu Siemens Healthineer
11:30AM - 12:00PM	<b>HIMSS Changemaker in Health Awards: 2026 HIMSS/ACCE Excellence in CE-IT Synergies Award: Samantha Jacques</b>		
12:00PM - 1:00PM	<b>LUNCH</b>		
1:00PM - 1:45PM	<b>The Learning Hospital: AI as a Partner in Clinical Engineering</b>	The phrase Artificial Intelligence (AI) stimulates the imagination and spans the spectrum of great societal progress and scientific discovery to fear of being outsourced by large language model chatbots or worse being subjugated like in science fiction movies. AI is rapidly transforming the healthcare technology landscape, reshaping how medical devices are managed, maintained, secured, and integrated into clinical workflows.  This presentation will explore how AI enhances medical device performance, supports predictive maintenance, strengthens cybersecurity, and improves patient safety. Key topics include foundational AI principles, machine learning in medical devices, data quality and interoperability, regulatory considerations, ethical challenges, and the evolving role of the clinical engineer in an AI enabled healthcare system. It will attempt to bridge the perspectives of clinical engineering, information technology, and frontline clinical practice—highlighting that no AI is risk-free and how collaboration across these domains is essential for safe and effective AI adoption.	Perry Kirwan Executive, Clinical Engineering eEquip - Center for Clinical Technology Management, Sutter Health
1:45PM - 2:00PM	<b>BREAK</b> <span style="float: right;"><b>Panelists</b></span>		
2:00PM - 4:00PM	<b>PANEL DISCUSSION: Future-Ready Healthcare: From Evolution to Revolution</b>	We will explore the pivotal question: are we on the brink of a revolutionary transformation, or perhaps it is just another stage of evolution? Discover the essential skills executives feel would help you be ready for the challenges ahead.	Mahesh Chintakunta Bill Riley Ernest Liu Perry Kirwan Phil Englert

# How Public/Private Partnerships can help you!

## Learn about the Health Sector Coordinating Council

Samantha Jacques, PhD, FACCE



# Meet our Speaker



Samantha Jacques, PhD, FACHE, FACCE, AAMIF  
Vice President, Corporate Clinical Engineering

Samantha Jacques, PHD, FACHE, FACCE, AAMIF is the Vice President of Clinical Engineering at McLaren Health. She manages medical technology throughout the McLaren System including 13 hospitals, ambulatory surgery centers, imaging centers, and Michigan’s largest network of cancer centers.

Prior to McLaren, she was Director of Clinical Engineering at Penn State Health and Texas Children’s Hospital. She is also Vice Chair of the Health Sector Coordinator Council – Cybersecurity where she advises the US Government on behalf of the health sector. She has previously sat on the Boards of Healthcare associations including AAMI and ACCE. She has also published a book titled “Introduction to Clinical Engineering” and adjunct teaches in the field of Cybersecurity.

She has a BS in Biomedical Engineering from Milwaukee School of Engineering and PhD in Biomedical Engineering from Louisiana Tech University.



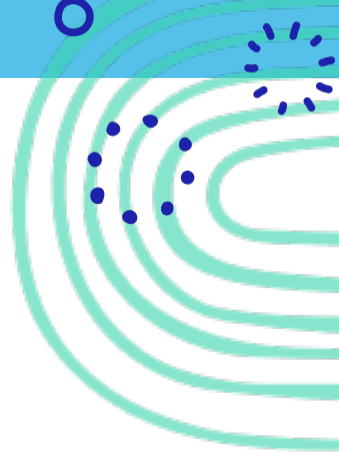
# Agenda

- Learn what is the Health Sector Coordinating Council – Cyber Working Group is.
- From obtaining free guidance on cutting edge issues to learning about how other organizations tackle challenges – come learn about what the Health Sector Coordinating Council Cybersecurity Working Group has to offer.
- Learn about our initiatives, best practice guidance, how we work to inform our government partners, and what we can do for you.

# Conflict of Interest

**Samantha Jacques**

has no real or apparent conflicts of interest to report.



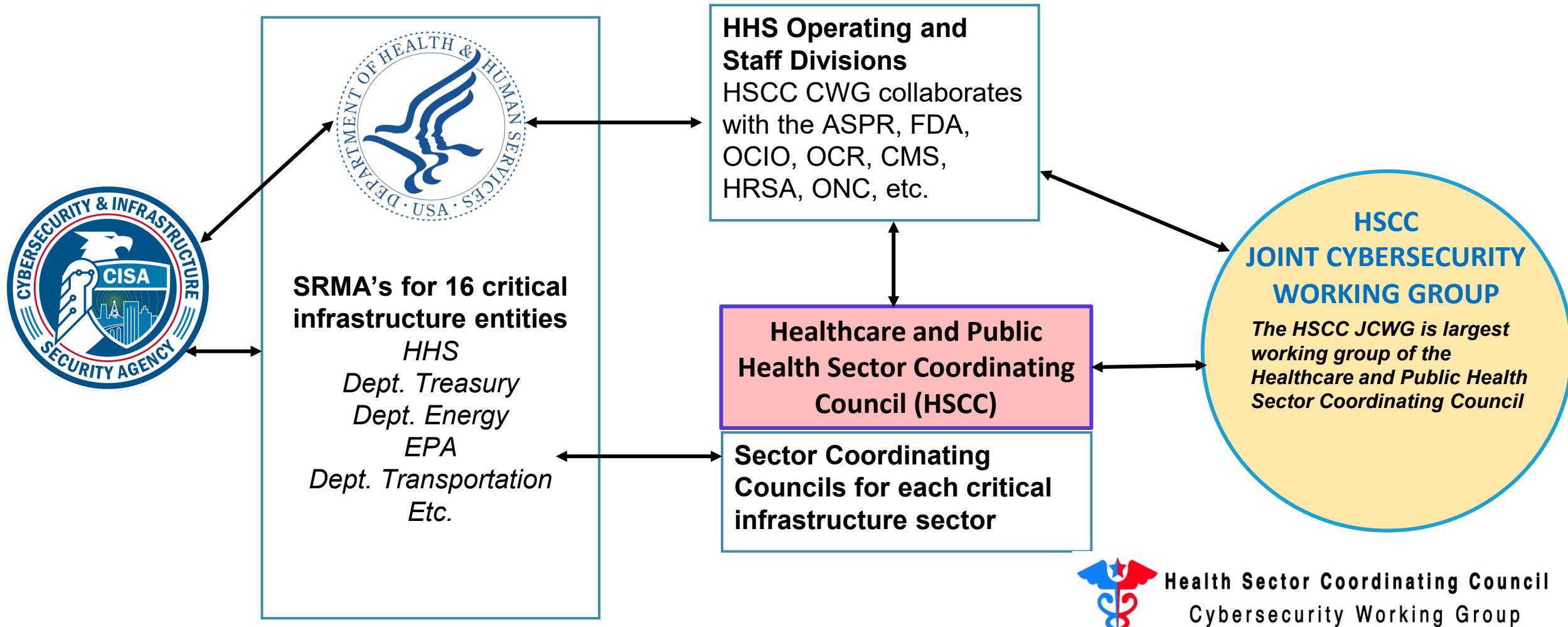
# HSCC Joint Cybersecurity Working Group (JCWG)

- Industry advisory council that is joined by government to identify and develop strategic, cross-sector solutions to cybersecurity threats and vulnerabilities affecting the security and resiliency of the healthcare sector
- Outcome-oriented task groups develop best practices; Full JCWG membership meets twice a year in person around the country
- Works closely on joint initiatives with
  - HHS Administration for Strategic Preparedness and Response
  - Food and Drug Administration
  - Other HHS Operating Divisions and DHS CISA



Health Sector Coordinating Council  
Cybersecurity Working Group

# Critical Infrastructure Protection Public Private Partnership



# The Health Sector - An Interconnected Ecosystem



## Laboratories, Blood & Pharmaceuticals

Pharmaceutical Manufacturers  
 Drug Store Chains  
 Pharmacists' Associations  
 Public and Private Laboratory Associations  
 Blood Banks

## Medical Materials

Medical Equipment & Supply Manufacturing & Distribution  
 Medical Device Manufacturers

## Health Information Technology

Medical Research Institutions  
 Information Standards Bodies  
 Electronic Medical Record System and Other Clinical Medical System Vendors

## Federal Response & Program Offices

Coordinated Response Activities Under Emergency Support Function 8  
 Government Coordinating Council  
 Federal Partners (e.g., HHS, DoD, other sector partners)

## Direct Patient Care

Healthcare Systems  
 Professional Associations  
 Medical Facilities  
 Emergency Medical Services  
 Consumer Devices \ BYOD

## Mass Fatality Management Services

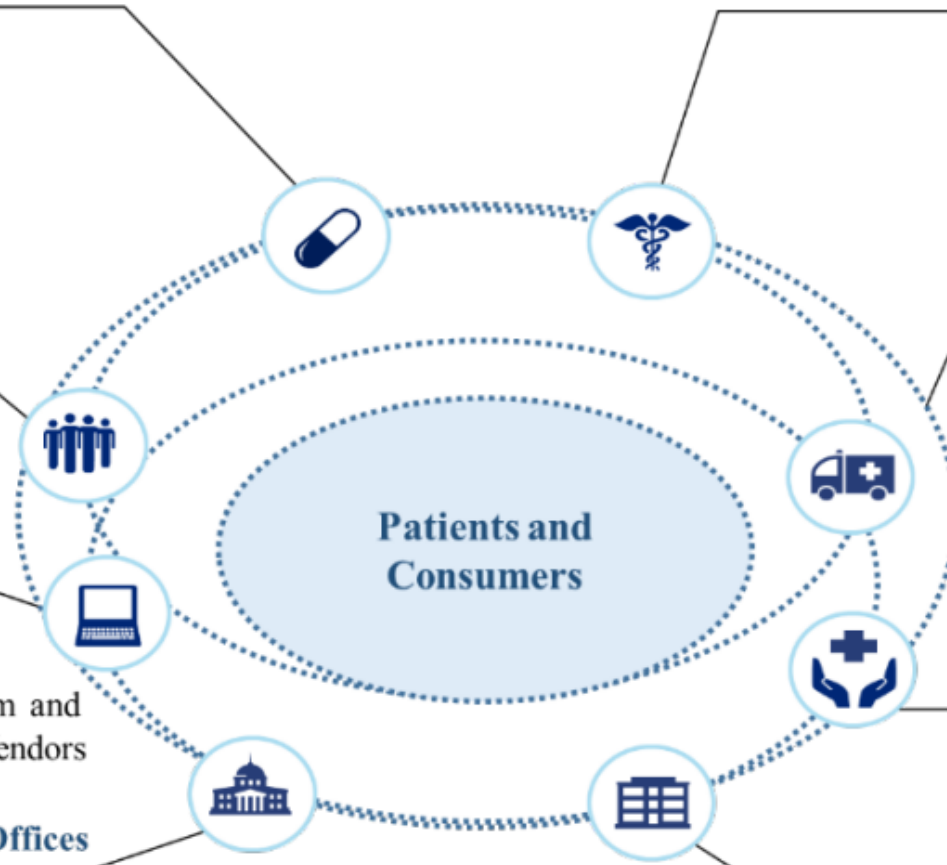
Cemetery, Cremation, Morgue, and Funeral Homes  
 Mass Fatality Support Services (e.g., coroners, medical examiners, forensic examiners, & psychological support personnel)

## Health Plans and Payers

Health Insurance Companies & Plans  
 Local and State Health Departments  
 State Emergency Health Organizations

## Public Health

Governmental Public Health Services  
 Public Health Networks



# Membership Eligibility

## Voting “Owner-Operator” Members

- Covered Entities and Business Associates involved in direct patient care subject to HIPAA
- Health plans and payers
- Medical materials, technology, and distribution subject to FDA regulation
- Pharmaceuticals, laboratories, blood entities subject to FDA regulation
- Health Information Technology owners, operators and manufacturers subject to interoperability rules
- Mass fatality management services
- Trade groups and professional societies representing any of the above
- Government (state, local, tribal, territorial, and federal)
- **Voting Members elect the CWG Executive Committee (which elects Chair and Vice Chair) and vote as requested on approval of publications and any other CWG decisions and positions**

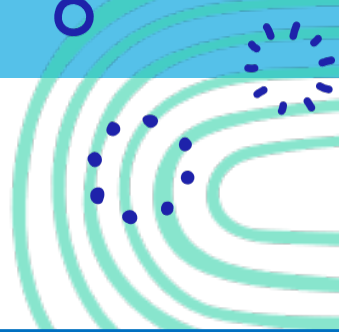
## Non-Voting Advisor Members

- Entities that are not regulated owner-operators of the healthcare system but that have healthcare, cybersecurity and/or healthcare cybersecurity-specific expertise as consultants, law firms, security companies
- Advisor organization membership is capped at 15% of the Voting Membership
- Advisors are asked to join at least one task group and participate in at least 50% of the task group’s meetings
- Advisors are asked not to engage in any business development/sales activities while participating in HSCC business as HSCC publications and communications cannot favor any vendor, technology or member relative to any other
- **Advisors neither vote nor hold CWG leadership positions, and join by invitation of leadership, subject to annual review.**

# 2026 Membership



Health Sector Coordinating Council  
Cybersecurity Working Group



- **458 private sector organizations, including:**
  - 410 Voting owner-operators Includes 58 industry associations and professional societies
  - 49 non-voting advisor companies
- **23 government organizations, including**
  - 11 federal
  - 6 state
  - 2 city
  - 2 county
  - 2 Canadian



*[Links to member list](https://healthsectorcouncil.org/about/organizational-members/)*

[https://healthsectorcouncil.org/about/  
organizational-members/](https://healthsectorcouncil.org/about/organizational-members/)

**Total Member**

**Personnel:**

**1076**

# Member Distribution by Subsector

- Direct Patient Care: **46.30%**
- Health Information Technology: **4.44%**
- Health Plans and Payers: **5.07%**
- Mass fatality and Management Services: **0**
- Medical Materials: **9.94%**
- Laboratories, Blood, Pharmaceuticals: **5.29%**
- Public Health: **4.44%**
- Cross-sector: **8.25%**
- Government (Fed, State, County, Local): **4.86%**
- Advisors: **10.15%**



Health Sector Coordinating Council  
Cybersecurity Working Group

# Cybersecurity Working Group 2026 Industry Executive Committee



## CHAIR

Chris Tyberg  
CISO  
ABBOTT  
*December 2026*



## VICE CHAIR

Samantha Jacques  
VP Corporate Clinical Engineering  
MCLAREN HEALTH CARE  
*December 2026*



## AT-LARGE

Dr. Jeff Tully  
Co-Director,  
Center for Healthcare Cybersecurity  
UC SAN DIEGO  
*December 2028*



## CROSS SECTOR

Bobby Rao  
CISO  
BAYER CROP SCIENCES  
*December 2026*



## DIRECT PATIENT CARE

James Case  
VP & CISO  
BAPTIST HEALTH NE FLORIDA  
*December 2027*



## DIRECT PATIENT CARE

Anahi Santiago  
CISO  
CHRISTIANACARE  
*December 2027*



## HEALTH IT

Paul Matthews  
CISO  
OCHIN, INC.  
*December 2026*



## MEDICAL TECHNOLOGY

Nimi Ocholi  
Vice President, R&D,  
Product Security  
BD  
*December 2028*



## PLANS-PAYERS

Rob Suarez  
VP & CISO  
CAREFIRST BLUECROSS  
BLUESHIELD  
*December 2028*



## PHARMA-LAB-BLOOD

Inhel Rekik  
Senior Director  
Product Security  
BRACCO GROUP  
*December 2027*



## PUBLIC HEALTH

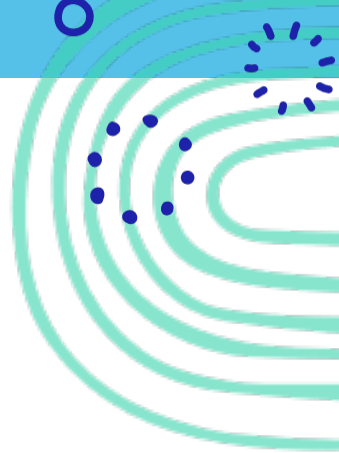
Dennis Small  
Chief Technology Officer  
NATIONAL ASSOCIATION OF CITY  
AND COUNTY HEALTH OFFICIALS  
*December 2028*



## OPERATIONAL LIAISON (non-voting)

Denise Anderson  
President & CEO  
HEALTH-ISAC  
*Continuity*

# JCWG Government Co-Chairs



## **Brian Mazanec**

**Deputy Assistant Secretary and Deputy Director  
Center for Preparedness  
Administration for Strategic Preparedness and Response**

## **Suzanne Schwartz**

**Director  
Office of Strategic Partnerships & Technology Innovation  
Center for Devices and Radiological Health  
U.S. Food and Drug Administration**

# Five-Year Health Industry Cybersecurity Strategic Plan (HIC-SP)



billy



Health Sector Coordinating Council  
Cybersecurity Working Group



Monitor  
Threats



Manage  
Risks



Respond &  
Recover



Measure  
Effectiveness

## Health Industry Cybersecurity – Strategic Plan (2024–2029)



FEBRUARY 2024

# Cybersecurity Strategic Plan Implementing Objectives

<b>01</b>	Develop, adopt and demand safety and resilience requirements for products and services offered, from business to business, as well as health systems to patients, with the concept of secure-by-design and secure-by-default	<b>07</b>	Increase incentives, development and promotion of health care cybersecurity-focused education and certification programs
<b>02</b>	Simplify access to resources and implementation approaches related to the adoption of controls and practices aligned with regulatory and sector standards for securing devices, services, and data	<b>08</b>	Increase utilization of automation and emerging technologies like AI to drive efficiencies in cybersecurity processes
<b>03</b>	Develop and adopt practical and uniform privacy standards to protect personal information and promote fair and ethical data practices while sharing the data in a consensual eco-system	<b>09</b>	Develop health sub-sector specific integrated cybersecurity profile aligned with regulatory requirements
<b>04</b>	Increase new partnerships with public/private entities on the front edge of evaluating and responding to emerging technology issues to enable safe, secure, and faster adoption of emerging technologies	<b>010</b>	Develop meaningful cross-sector third-party risk management strategies for evaluating, monitoring, and responding to supply chain and third-party provider cybersecurity risks
<b>05</b>	Enhance health sector senior leadership and board knowledge of cybersecurity and their accountability to create a culture of security within their organizations	<b>011</b>	Increase meaningful and timely information sharing of cyber related disruptions to improve sector readiness
<b>06</b>	Increase utilization of cybersecurity practices / resources / capabilities by public health, physician practices and smaller health delivery organizations (e.g., rural health)	<b>012</b>	Develop mechanisms to enable “mutual aid” support across sector stakeholders to allow for timely and effective response to cybersecurity incidents

# 2029 Target Future State

If we succeed, the diagnosis of healthcare cybersecurity will upgrade from “Critical Condition” in 2017 to “Stable Condition” in 2029. “Cyber Safety is Patient Safety” will be characterized by:



<b>Reflexive Cybersecurity</b>	<b>Secure Design &amp; Implementation</b>	<b>C-Suite Ownership</b>	<b>Cyber Safety Net</b>	<b>Cyber Competence</b>	<b>911 Cyber Civil Defense</b>
<p>Both practiced and regulated healthcare cybersecurity is reflexive, evolving, accessible, documented and implemented for practitioners and patients.</p>	<p>Technology and services across the healthcare ecosystem is a shared and collaborative responsibility.</p>	<p>Healthcare C-Suite embraces accountability for cybersecurity as enterprise risk and a technology imperative.</p>	<p>Under-resourced health organizations are supported in the form of financial, policy and technical assistance ensuring cyber equity across the ecosystem.</p>	<p>Workforce learning and application is an infrastructure wellness continuum.</p>	<p>Ensures that early warning, incident response and recovery are reflexive, collaborative and always on.</p>



# HSCC Joint Cybersecurity Working Group 2026 Task Groups Objectives And Leadership

TASK GROUP	OBJECTIVE	INDUSTRY LEADS	GOVT. LEAD
Artificial Intelligence Cybersecurity	Identify the emerging risks associated with the use of AI/ML based products and services in HPH and develop recommendations for their mitigations. Develop guidelines, standards, and best practices for AI safety and security.	Rohit Tandon – Essentia Health	HHS ASPR-
		Rob Suarez – CareFirst	Charlee Hess
Cybersecurity Board Governance	Develop initiative(s) to enhance health sector senior leadership and board knowledge of cybersecurity and accountability to create a culture of security within their organizations	Inhel Rekik – Bracco Group	N/A
		Janine Fadul – George Washington University	
		Bill Reid – Google	
Health Industry Cybersecurity Landscape Analysis	Update 2023 Hospital Cybersecurity Landscape Analysis which identified the vulnerabilities and threats most frequently resulting in damaging attacks against hospitals and assesses the hospitals’ known capabilities for preventing damaging cyber incidents. Version 2 of the L.A. will incorporate more data in the analysis and consider vulnerabilities and incidents faced by additional subsectors.	Anahi Santiago – ChristianaCare	HHS ASPR-
		James Case – Baptist Health NE Florida	Charlee Hess
		Ron Mehring – Texas Health Resources	
MedTech Cybersecurity Updating/Patching	Develop mutual expectations among health delivery organizations and medical device manufacturers about updating and patching medical devices in the clinical environment, and associated risk, prioritization and cost.	Chris Gates – arsMedSecurity	HHS FDA –
		Phil Englert – Health ISAC	Lisa Gilbert
MedTech Manufacturing OT Cybersecurity	Developing leading practices for cybersecurity management of operational/manufacturing technology. Initially focused on medical technology and pharmaceutical subsectors.	Tyrone Heggins, Becton Dickinson Erin Gilliam – Merck	TBD



# HSCC Joint Cybersecurity Working Group 2026 Task Groups Objectives And Leadership

TASK GROUP	OBJECTIVE	INDUSTRY LEADS	GOVT. LEAD
<b>MedTech Vulnerability Communications</b>	Provide guidance to differing stakeholders (MDMs, HDO's, clinicians, patients) on preparing, receiving and acting on medical device vulnerabilities. First publication April 2022 on patient awareness. Second version on HDO/MDM engagement and implementation in process.	Les Gray, Abbott  (Advisor) Axel Wirth - Medcrypt	TBD
<b>Outreach and Awareness</b>	Develop CWG brand and marketing strategy	Kristi Warner – Abbott	TBD
<b>Post Quantum Cryptography</b>	Develop <ul style="list-style-type: none"> <li>Shared cryptographic asset inventory framework for organizations to baseline their current exposure.</li> <li>Cross-industry roadmap for PQC migration, including interoperability and supply-chain considerations.</li> <li>Guidelines and reference architectures for pilot implementations and vendor engagement.</li> <li>Recommendations for regulatory and compliance alignment to support smooth adoption across industries.</li> </ul>	TBD	TBD
<b>Public Health Cybersecurity</b>	Identify strategies for strengthening the cybersecurity and resilience of SLTT public health agencies with the support of private sector and academic organizations.	Dr. Leanne Field – The UT Austin	HHS ASPR – <b>Bob Bastani</b>
<b>Underserved Provider Cybersecurity Advisory Group</b>	Conduct a series of documented panel discussions with management of under-resourced providers to interview for perspectives about cybersecurity challenges, financial and operational challenges, and their needs for assistance to meet cybersecurity obligations	Jennifer Stoll – OCHIN, Inc.  Jim Roeder – Lakewood Health System	TBD

# Best Practices and Recommendations





# Publications (34)

## By the Sector for the Sector

### 2025

- [Medtech Model Cybersecurity Contract v2](#)
- [A.I. Cybersecurity One-Pagers](#)
- [Sector Mapping and Risk Toolkit](#)
- [On the Edge: Cyber Health of Resource-Constrained](#)
- [Cybersecurity Consultative Process Proposal](#)
- [Recommendations for Government Policy and Programs](#)

### 2024

- [Medical Product Manufacturer Cyber Incident Response Playbook](#)
- [Executive Checklist for Incident Response](#)
- [Medical Device and Health IT Joint Security Plan v2 \(JSP2\)](#)
- [Health Industry Cybersecurity Strategic Plan](#)
- [Coordinated Privacy Security Partnerships](#)

### 2023

- [Health Industry Cybersecurity Information Sharing Best Practices](#)
- [Health Industry Cybersecurity Matrix of InfoSharing Organizations](#)
- [Coordinated Healthcare Incident Response Plan](#)
- [Recommended Government Policy & Programs](#)
- [Hospital Cyber Landscape Analysis \(Joint HSCC/HHS\)](#)
- [Prioritized Recognized Cybersecurity Practices](#)

- [Cybersecurity for Clinician Video Training Series](#)
- [Health Industry NIST CSF Implementation Guide \(Joint\)](#)
- [Managing Legacy Technology Security](#)
- [Artificial Intelligence Machine Learning](#)

### 2022

- [Operational Continuity-Cyber Incident Checklist](#)
- [MedTech Vulnerability Communications Toolkit](#)
- [Model Contract-Language for Medtech Cybersecurity](#)

### 2021

- [Securing Telehealth and Telemedicine](#)

### 2020

- [Supply Chain Risk Management](#)
- [Health Sector Return-to-Work Guidance](#)
- [Tactical Crisis Response](#)
- [Protection of Innovation Capital](#)
- [Checklist for Teleworking Surge During COVID-19](#)

### 2019

- [Workforce Guide](#)
- [Medical Device and Health IT Joint Security Plan](#)
- [Health Industry Cybersecurity Practices \(Joint\)](#)



*Link to  
publications*

# Cyber Practices

By the Sector, For the Sector

How our resources are organized  
on <https://HealthSectorCouncil.org>

You're a health provider, medical technology or health I.T. company, pharmaceutical manufacturer, health plan or payer, public health agency.

How do you want to improve your cybersecurity posture?



## Monitor Threats

- > [Health Industry NIST CSF Implementation Guide](#)
- > [Artificial Intelligence Machine Learning](#)
- > [Health Industry Cybersecurity Practices 2023](#)
- > [Health Industry Cybersecurity Supply Chain Risk Management Guide \(HIC-SCRiM-2023\)](#)

VIEW MORE



## Manage Risks

- > [Health Industry Cybersecurity - Coordinated Privacy Security Partnerships \(HIC-CPSP\)](#)
- > [Health Industry Cybersecurity - Securing Telehealth and Telemedicine \(HIC-STAT\)](#)
- > [Health Industry Cybersecurity - Matrix of Information Sharing Organizations \(HIC-MISO\)](#)
- > [Prioritized Recognized Cybersecurity Practices](#)

VIEW MORE



## Respond & Recover

- > [Health Industry Cybersecurity Tactical Crisis Response Guide \(HIC-TCR\)](#)
- > [Health Industry Cybersecurity - Matrix of Information Sharing Organizations \(HIC-MISO\)](#)
- > [Coordinated Healthcare Incident Response Plan \(CHIRP\)](#)
- > [Health Industry Cybersecurity Practices 2023](#)

VIEW MORE



## Measure Effectiveness

- > [Health Industry Cybersecurity - Matrix of Information Sharing Organizations \(HIC-MISO\)](#)
- > [Hospital Cyber Landscape Analysis \(Joint HSCC/HHS\)](#)



## Secure Medtech

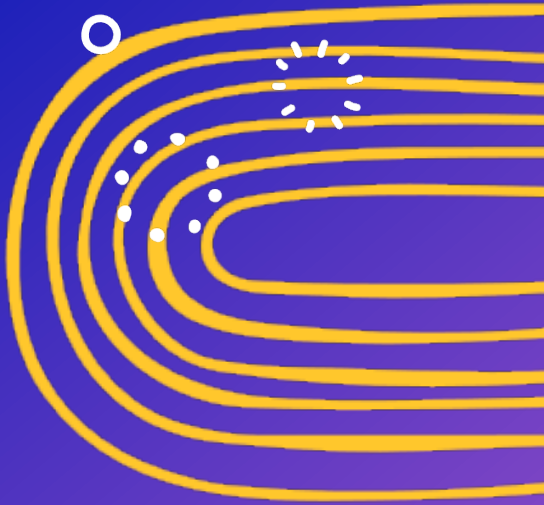
- > [Medical Device and Health IT Joint Security Plan version 2.0 \(ISP2\)](#)
- > [Medtech Vulnerability Communications Toolkit \(MVCT\)](#)

# How to get involved?

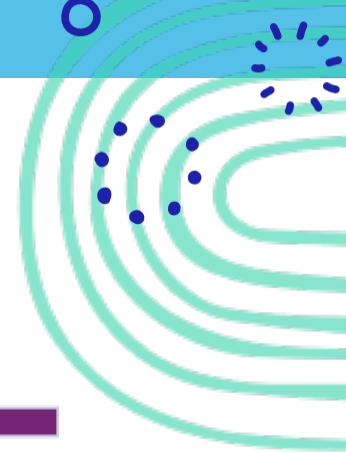
Greg Garcia – Executive Director  
[Greg.Garcia@healthsectorcouncil.org](mailto:Greg.Garcia@healthsectorcouncil.org)

Healthsectorcouncil.org





# Questions



9:40AM - 10:30AM	<b>Uncovering 'Invisible' Medical Devices: How a cyber ecosystem can help</b>	An ecosystem of cybersecurity tools helped improve the visibility of a hospital system's connected medical devices by 60%. This is achieved by integrating cybersecurity tools with a medical device security management platform (MDSM) over a few quarters. This largely helped to understand the risks associated with the hospital and provided an opportunity to address them.
------------------	---	---



# UNCOVERING 'INVISIBLE' DEVICES

*How a Cyber Ecosystem Can Help*

---

**Mahesh Chintakunta**

Sr. Director, Cybersecurity Operations & Engineering | RUSH



# Meet our Speaker

## Professional Overview

- 20+ years of IT experience, including 15+ years in cybersecurity
- Leads cybersecurity operations and engineering at RUSH
- Founded and scaled the Medical Device Security Program at RUSH

## Expertise

- Security Operations & Vulnerability Management
- Medical Device & Clinical Cybersecurity
- Cloud Security & Enterprise Architecture
- Managed Security Services (Fortune 100)

## Thought Leadership

- Author of several published cybersecurity articles
- Frequent speaker and security awareness advocate

Mahesh lives in Naperville with his wife, Srujana, and two sons, Yash and Srimaan. He volunteers in local non-profit organizations and teaches Yoga for free. He has been teaching yoga at multiple schools for the last two years.



**Mahesh Chintakunta**  
Sr. Director, Cybersecurity Operations  
& Engineering at Rush

RUSH UNIVERSITY SYSTEM FOR  
HEALTH

# Agenda

An ecosystem of cybersecurity tools helped improve the visibility of a hospital system's connected medical devices by 60%.

This is achieved by integrating cybersecurity tools with a medical device security management platform (MDSM) over a few quarters.

This largely helped to understand the risks associated with the hospital and provided an opportunity to address them.



Founded in 1837



3 Hospitals and 30+ Clinics



671 beds



Hospital + Research  
+ Medical University



40



6+

*~3 years ago, the team was tracking 5,800 connected medical devices — yet knew many more remained invisible.*

**01**

### **Limited Visibility**

The MDSM platform was not configured for active scanning or discovery — leaving thousands of devices undetected on the network.

**02**

### **Cannot Locate Device (CNL)**

Multiple 'Couldn't Locate the Device' incidents plagued service providers, creating operational delays and patient safety risks.

**03**

### **Poor Utilization Data**

Insufficient network intelligence meant device utilization rates were sub-optimal — undermining capital investment decisions.

*"There were several additional challenges with vulnerability and risk management because of a lack of visibility."*

*By integrating cybersecurity tools into the MDSM platform, the team ingested the network intelligence needed to conclusively identify medical devices.*

## 1. SNMP

Wireless LAN controllers →  
MAC address, SSID, AP model,  
location, serial, SW version

## 2. DNS

Enhanced device parameters:  
MAC, hostname, IP, OS, VLAN  
ID & description

## 3. Infrastructure Vulnerability Scanner

Mapped CVE information directly  
to devices in the platform

## 4. EDR

1M+ detections visible;  
combined network & endpoint  
risk in a single pane

## 5. Network Mgmt Tools

MAC address, logical location,  
IP, model, hostname, SW  
version, serial, location

## 6. Vendor CMDB

Device utilization data sent to  
CMDB — key input for capital  
committee decisions

★ Integration #6 (Vendor CMDB) is external to the hospital network — all others operate within it.

# 60%

## BOOST IN DEVICE VISIBILITY

by integrating cybersecurity  
tools with the MDSM platform

### BEFORE INTEGRATION



5,800 devices tracked

### AFTER INTEGRATION



9,300+ devices tracked (3,000+ newly discovered)

- Device Visibility:** MDSM now conclusively identifies thousands more medical devices
- Device Utilization:** Vendor CMDB integration enables reliable capital investment decisions
- Risk Management:** CVE data + EDR detections combined in a single pane for faster response

*Note: Sharp rise after DNS integration reflects the cumulative effect of all prior integrations combined.*

## INVENTORY AND VISIBILITY

- We NOW have a consolidated inventory of IoT and IoMT devices while finding "unmanaged" devices
- We use passive scanning and vuln scanner data to discover all device, apps, services, and connections

## VULNERABILITY PRIORITIZATION & REMEDIATION

- Because of a thorough inventory, we can identify and prioritize the 2% riskiest devices in the environment for immediate risk reduction
- We use a risk simulator to identify perceived effort for any given action before remediation

# An Integrated MDSM Ecosystem

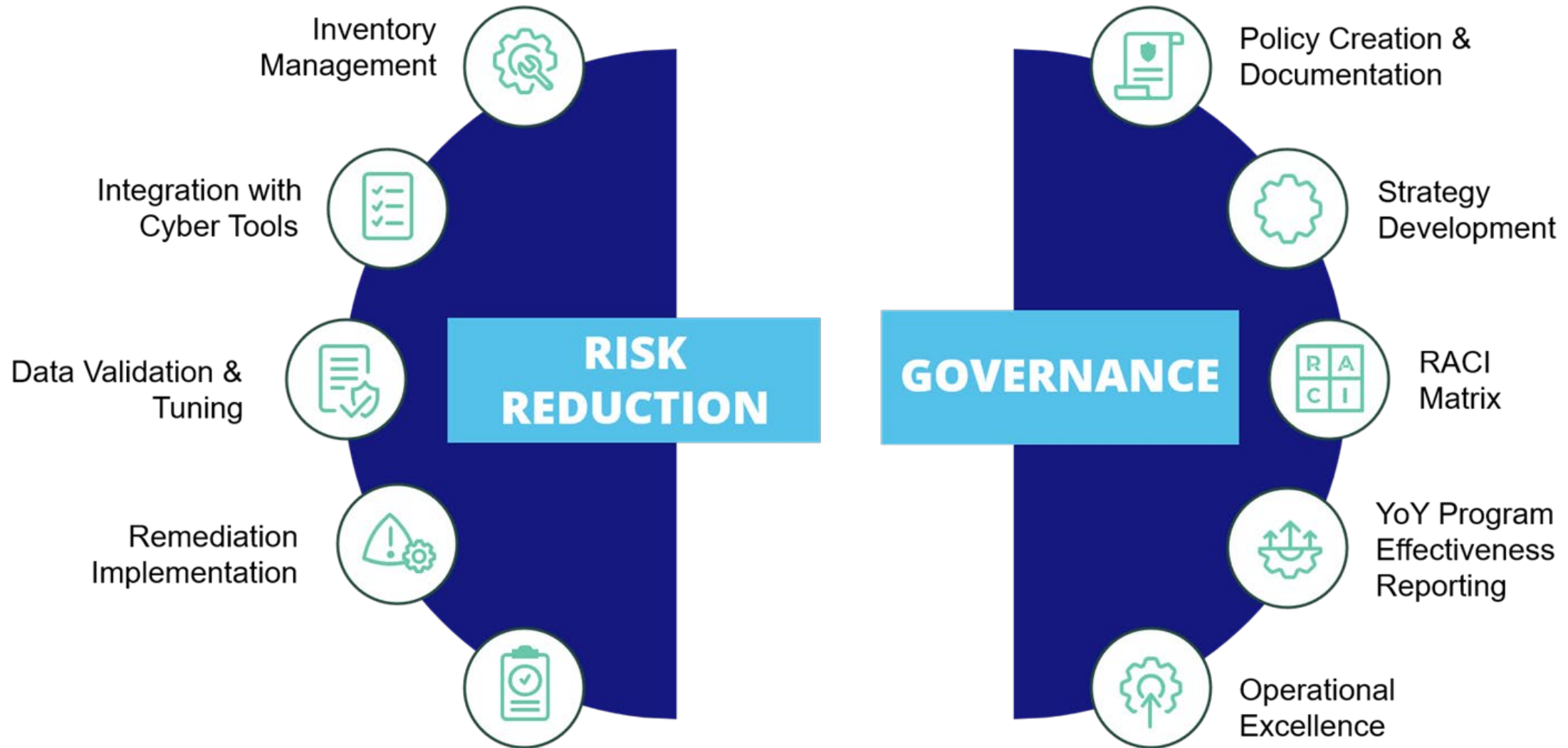


## MSDM DATA NORMALIZED IN SIEM

- MSDM data is normalized, correlated and consolidated in our SIEM
- This makes it easier to prioritize defensive actions, spot anomalies, provide reports for compliance, and ensure there are no unmanaged cyber assets in the entire network.

## THREAT AND RESPONSE

- We set intelligent policies to thwart known exploits from spreading to additional devices
- We automate packet capture for forensic analysis of any connected device to support root cause analysis and reduce Incident Response costs



# What Healthcare Organizations Can Learn



## Visibility is foundational

You can't secure what you can't see. Before tackling vulnerability management, confirm your MDSM platform has the network intelligence to conclusively identify every device.



## Integrate to illuminate

No single tool is enough. SNMP, DNS, EDR, network scanners, and CMDB working in concert resolved all three challenges — device visibility, CNL incidents, and utilization data.



## Be strategic — not exhaustive

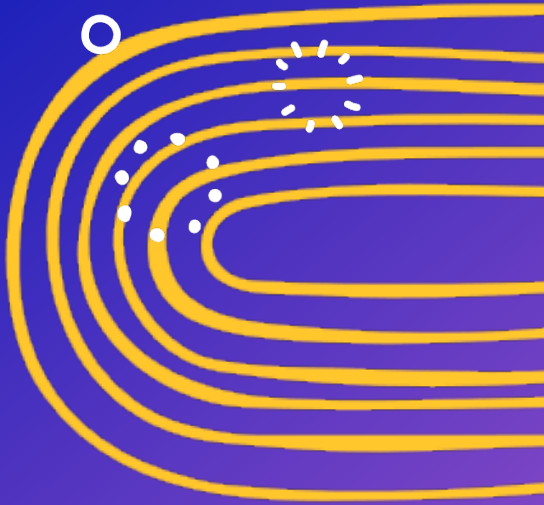
There were too many tools to integrate at once. Prioritizing by discovery capability, telemetry sharing, ease of integration, and cost kept the effort focused and successful.



## Security data drives business decisions

The vendor CMDB integration delivered reliable utilization rates — giving the capital investment committee the data they need to justify and prioritize equipment spending.

*"Healthcare providers can use their current cybersecurity setup to enhance patient safety, improve resource use, and foster robustness in an increasingly connected medical landscape."*



# Questions

# Advancing Secure, IT-Ready Medical Devices

## *A Collaborative Evaluation Model*

Educational session • Non-production evaluation • No endorsement

Bill Riley

Ernest Liu



# Agenda

Healthcare Delivery Organizations (HDOs) increasingly need medical devices that integrate seamlessly with modern cybersecurity and network management tools. Mayo Clinic's HTM program has been advocating for this shift, pressing manufacturers to design equipment that functions more like contemporary IT assets. Many manufacturers have expressed concerns about feasibility, risk, and regulatory complexity—but Siemens has become the first to break new ground.

In this session, Siemens will demonstrate a next-generation ultrasound platform engineered to operate within standard IT frameworks, enabling native compatibility with enterprise cybersecurity controls, patching workflows, and endpoint management tools. Mayo Clinic will share how both organizations collaborated to test, validate, and prove these capabilities in real clinical and technical environments.

## Meet our Speaker



William (Bill) Riley,  
Sr. Information Security Engineer

- **William (Bill) Riley** is a Senior Information Security Engineer in Healthcare Technology Management at Mayo Clinic, with more than 28 years in systems management and medical device cybersecurity. He works at the intersection of HTM, enterprise security, and device manufacturers to strengthen secure lifecycle practices for connected medical equipment.

## Meet our Speaker



Ernest Liu,  
Cybersecurity & Product Security Manager

- Americas Regional Cybersecurity & Product Security Manager at Siemens Healthineers, with over 25 years of experience spanning cybersecurity, product management, and enterprise diagnostic imaging integration. He specializes in securing network-connected medical equipment through standardized onboarding, vulnerability management, and enterprise-scale risk remediation.
- Specialist in medical device and IoMT cybersecurity, focused on securing network-connected imaging systems, regulatory alignment, and enterprise risk management across all Siemens imaging modalities.
- Trusted partner to healthcare providers and clinical engineering teams, translating cybersecurity risk into practical, customer-facing solutions that protect patient data and ensure secure device lifecycles.

# Session Roadmap (35 minutes)

- The IT-Ready Vision & Industry Reality
- Execution Models & Guardrails
- Platform Design & Evaluation Findings
- Decision Gate & Takeaways
- Q&A

# Defining IT-Ready

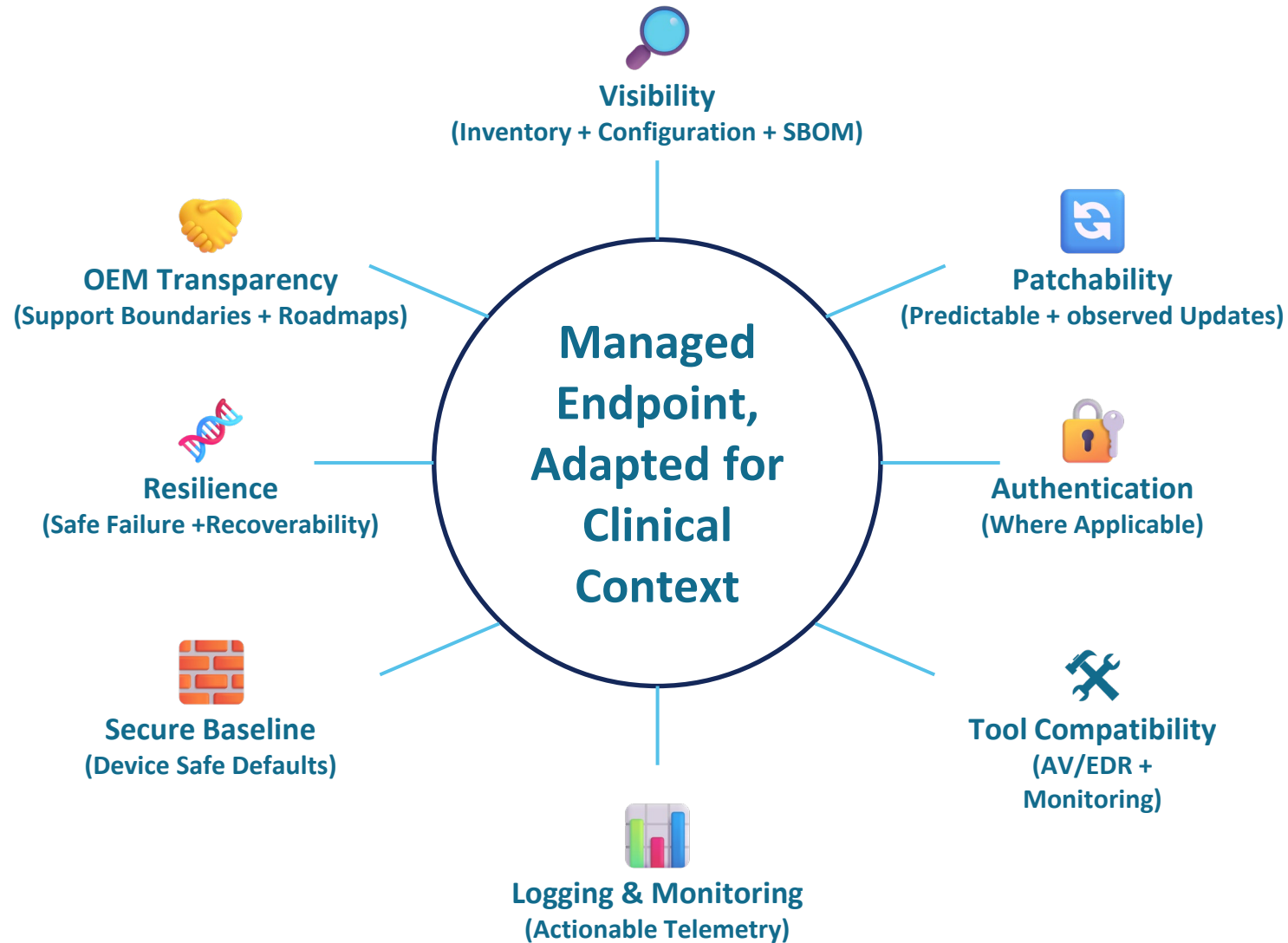
What It Is — and What It Is Not Meant to Be

## IT - Ready Is NOT

- Converting devices into generic IT assets
- Imposing identical support models
- Trading clinical safety for automation

## IT - Ready IS

- Operational Visibility
- Predictable lifecycle alignment
- Defined participation in enterprise identity
- Safe, governed enterprise integration

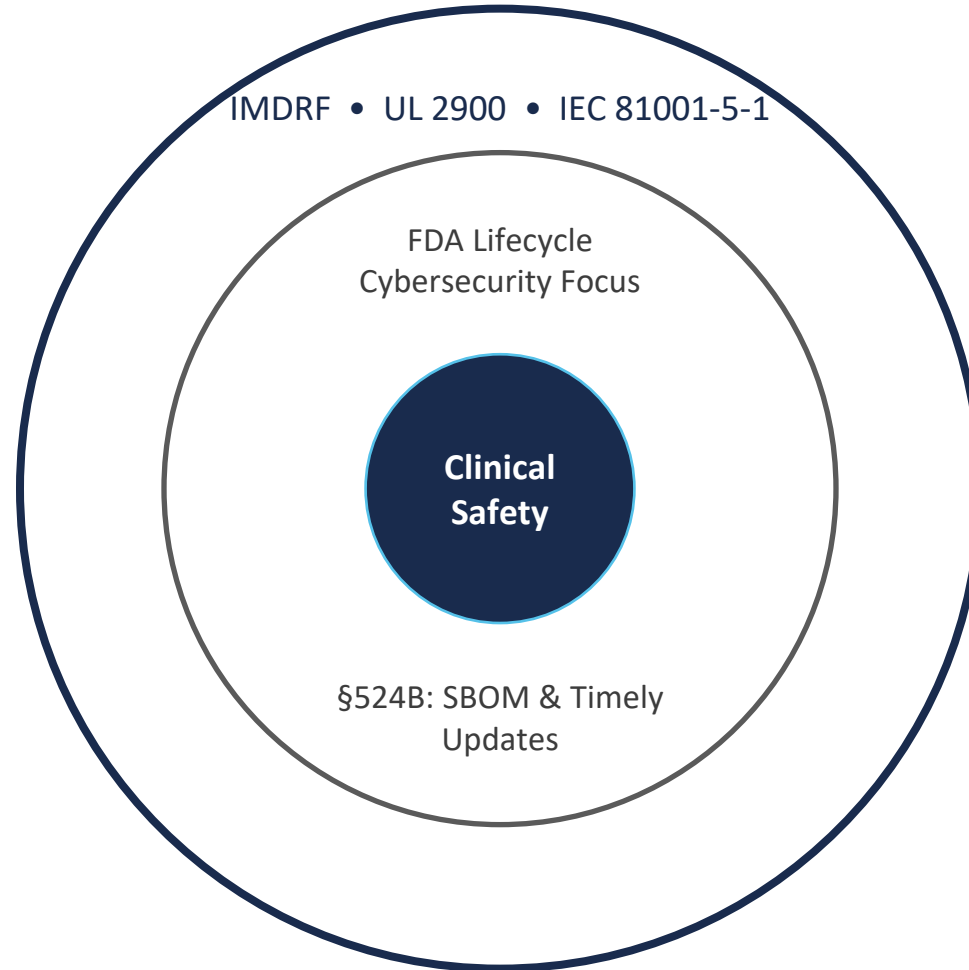


**HDO expectations:** visibility, predictability, identity participation, enterprise compatibility.  
**FDA guidance:** lifecycle outcomes — not specific tools.

# Industry Reality

- Legacy designs optimized for isolated reliability
- Enterprise environments demand identity-driven resilience
- OEM constraints: safety, legacy platforms, global markets, long lifecycles

# Regulatory & Standards Guardrails



Innovation operates within guardrails to protect clinical safety.

# Two Defensible Execution Paths

## Model A

*HDO - Orchestrated*  
Manufacturer-observed

- Internal deployment
- Prescribed cadence
- HTM validation authority

## Model B

*Manufacturer-Managed*  
HDO – observed

- Direct patch execution
- Defined oversight
- Clinical safety gate

Both meet §524B when validation authority and accountability are explicit.

❤️ Patient Safety 📊 Operational Scalability 🕒 Timely Patch Availability

Scalable security. Preserved accountability. Protected patient safety

# Clinical & Enterprise Operating Principles

## Clinical Governance

- Clinical safety determines patch timing — not tooling convenience
- Manufacturer validation required for patches, agents, and configuration changes
- Regulatory accountability defined prior to execution

## Enterprise Guardrails

- Devices excluded from default enterprise automation without validation
- Deterministic allow-listing preferred over disruptive controls

## Risk Ownership

- Risk acceptance remains internal, documented, and accountable

**Applies Regardless of Execution Model**

# Collaboration Model

Enterprise Integration Framework for Medical Technology

<b>Structured Evaluation Environment</b> <ul style="list-style-type: none"><li>• Non-production evaluation lane</li><li>• Representative enterprise controls</li></ul>	<b>Collaborative Iteration</b> <ul style="list-style-type: none"><li>• Document observed behaviors</li><li>• Iterate jointly</li></ul>
<b>Clear Operational Boundaries</b> <ul style="list-style-type: none"><li>• Not a compliance scorecard</li><li>• Not a procurement gate</li></ul>	<b>Core Security Lifecycle Domains</b> <ul style="list-style-type: none"><li>• Patchability</li><li>• Baseline hardening</li><li>• Authentication</li><li>• Logging</li><li>• Resilience</li></ul>

Governed Collaboration — Not Certification or Endorsement

# Operational Expectations for Medical Technology

## Defined Support Boundaries

Clear articulation of:

- What configurations and controls can be safely modified
- What changes require OEM validation or coordination
- Shared accountability for lifecycle security management

## Enterprise Integration & Testing

Collaborative evaluation to ensure:

- Controlled coexistence with enterprise security controls
- Safe integration within the healthcare IT environment

## Operational Visibility

Telemetry and logging capabilities that support:

- Incident detection and response
- Enterprise monitoring and audit requirements

# Siemens: Platform Intent

- Reduce operational friction in enterprise environments
- Preserve clinical performance under security controls
- Align to lifecycle cybersecurity principles
- Translate HDO operational requirements into explicit device behaviors
- Represents an early example of observed enterprise participation in this device class

Clarification: This Siemens example is provided solely to illustrate application of the evaluation model in a non-production setting and does not imply exclusivity, preference, endorsement, or procurement guidance.

# Observed Through Structured Evaluation, non-production evaluation

- Patch cadence aligned to enterprise change windows
- Logging and authentication behaviors observed against defined enterprise criteria
- Coexistence with segmentation and monitoring confirmed
- Governance model applied throughout evaluation activities
- Observed compatibility with enterprise endpoint management workflows (where supported)

# Siemens: Updates & Patchability

- Documented patch cadence and update contents
- Clear impact documentation to support change planning
- Defined rollback procedures
- Observed alignment with defined enterprise change windows during evaluation

# Siemens: Logging & Monitoring

- Authentication, update, and system event exposed
- Log export capability with synchronized time
- Reduced operational blind spots
- Enables integration with enterprise monitoring workflows

# What Was Different

Engineered to participate in standard enterprise workflows — not operate as an exception.

- Enterprise-aligned patch cadence
- Authentication events exposed to enterprise logging
- Log export capability with synchronized time
- Explicit rollback procedures defined
- Identity participation observed in testing

Observed enterprise participation during non-production evaluation — not theoretical compatibility.

# Joint Findings + Discussion Scenarios

What worked immediately — and what required tuning  
Common tuning themes: default services, auth-failure behavior, update communication clarity

## Scenario A — Hybrid Governance Success

- OEM-observed bundle
- IT orchestration
- HTM downtime gate

## Scenario B — Speed Without Governance

- Automated OS patch
- Breaks a critical service during clinic hours

**What governance made A safe — and what control failed in B?**

# Guardrails & HTM Decision Gate

(All decisions require local clinical, HTM, and regulatory validation.)

No universal endorsements

Not a one-size-fits-all template

Site-specific validation is required

## Decision Gate — All Conditions Must Be Met

- Safety impact assessed
- OEM validation confirmed
- Owner identified
- Rollback plan defined

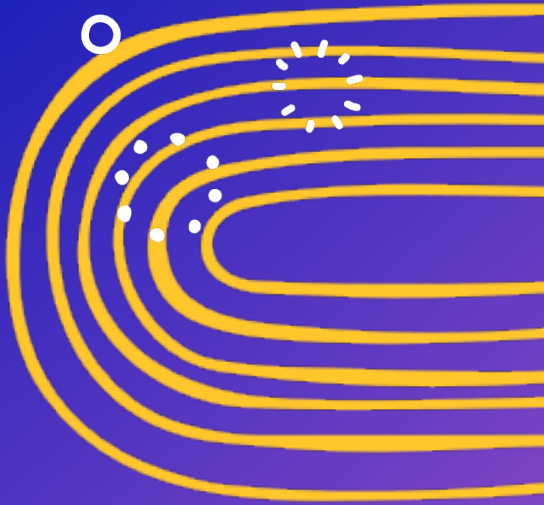
If any condition is unmet: apply compensating controls and defer change

**IT-readiness is a lifecycle attribute — not a bolt-on.**

# Reusable Playbook for IT-Ready Integration

## Operational Discipline

- No universal endorsements
- IT-readiness is a lifecycle attribute
- Governed and validated locally
- Align early • Evaluate safely • Publish support boundaries
- Regulation defines the floor — not the ceiling
- Designed into the lifecycle — not layered on afterward



# Questions

# Q&A (10 min) — Seed Questions

- How does your organization define and govern “IT-readiness” as a lifecycle attribute, rather than a one-time technical check?
- Where in your environment does early alignment break down today — and what governance signal would catch it sooner?
- What does a safe, structured evaluation lane look like in your organization, and who owns the decision to move out of it?
- How do you make support boundaries explicit before introducing enterprise controls or automation?
- When a change gate condition can’t be met, how do you decide between deferring change versus applying compensating controls?
- How do you use regulation and standards as anchors, without treating them as the ceiling for operational maturity?
- What would need to change — culturally or operationally — to design IT-readiness into the lifecycle instead of layering it on later?

# The Learning Hospital: AI as a Partner in Clinical Engineering

Perry Kirwan



# Meet our Speaker



Perry Kirwan, MEng  
Executive Director, Clinical Engineering



Perry Kirwan is currently the Executive Director at Sutter Health headquartered in Sacramento, CA. Sutter has 24 acute care facilities and well over 600 off-site locations that include outpatient imaging centers, ambulatory surgery centers, urgent care facilities, clinics and physician practices. The program supports over 150,000 assets in inventory.

Prior to Sutter Health, Perry was Vice President of Technology Management/ENTECH for Banner Health. He held several other leadership roles there over 30 years building new programmatic capabilities in capital planning/procurement, medical physics, asset management, service delivery/quality management, equipment standardization/new technology assessment, medical device integration, cybersecurity, and virtual reality.

He holds a BS in Cellular & Molecular Biology and BSE and MSE in Biomedical Engineering from Arizona State University and has published and lectured extensively over the years in topics of Healthcare Technology Management.

# SYNOPSIS

The phrase Artificial Intelligence (AI) stimulates the imagination and spans the spectrum of great societal progress and scientific discovery to fear of being outsourced by large language model chatbots or worse being subjugated like in science fiction movies. AI is rapidly transforming the healthcare technology landscape, reshaping how medical devices are managed, maintained, secured, and integrated into clinical workflows.

This presentation will explore how AI enhances medical device performance, supports predictive maintenance, strengthens cybersecurity, and improves patient safety. Key topics include foundational AI principles, machine learning in medical devices, data quality and interoperability, regulatory considerations, ethical challenges, and the evolving role of the clinical engineer in an AI enabled healthcare system. It will attempt to bridge the perspectives of clinical engineering, information technology, and frontline clinical practice—highlighting that no AI is risk-free and how collaboration across these domains is essential for safe and effective AI adoption.

# AGENDA

- AI FOUNDATIONS AND TRANSFORMATION IN HEALTHCARE
- AI IN MEDICAL DEVICES AND PREDICTIVE MAINTENANCE
- CYBERSECURITY, INTEROPERABILITY, AND REGULATORY FRAMEWORKS
- ETHICAL CONSIDERATIONS, CLINICAL ENGINEERING ROLE AND FUTURE TRENDS



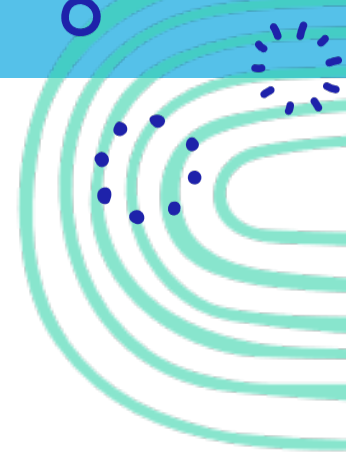
# THE LEARNING HOSPITAL: AI AS A PARTNER IN CLINICAL ENGINEERING

Enhancing healthcare through AI-driven clinical engineering

Perry Kirwan

Executive, Clinical Engineering

Sutter Health



# AI FOUNDATIONS AND TRANSFORMATION IN HEALTHCARE

# TRANSFORMATION OF HEALTHCARE THROUGH AI



## AI Automation and Augmentation

AI automates routine healthcare tasks and augments complex human decision-making using pattern recognition.

## Real-Time Data Analysis

AI analyzes large device data in intensive care units, enabling smarter maintenance and faster troubleshooting.

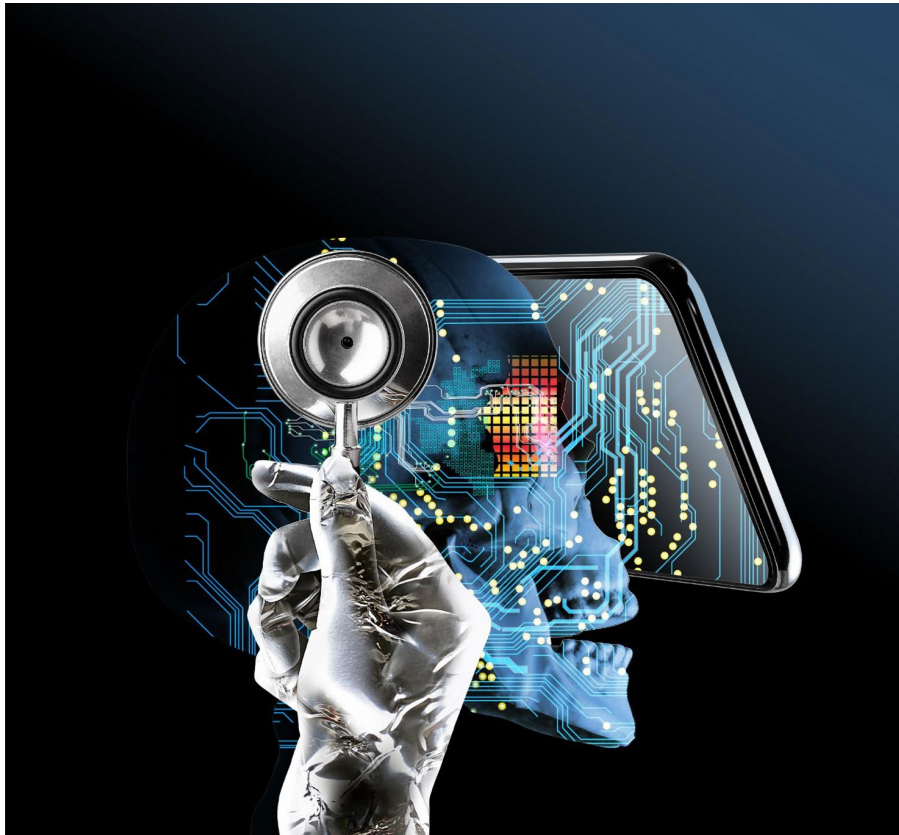
## Improved Patient Safety

AI reduces errors by detecting anomalies in infusion pumps, imaging diagnostics, and adaptive ventilators.

## System-Level Integration

AI fosters interoperability between health records, devices, cybersecurity, and hospital infrastructure for learning systems.

# FOUNDATIONS OF AI FOR CLINICAL ENGINEERING



## Core AI Disciplines

AI includes machine learning, deep learning, natural language processing, and rule-based systems vital for clinical engineering.

## Machine Learning Applications

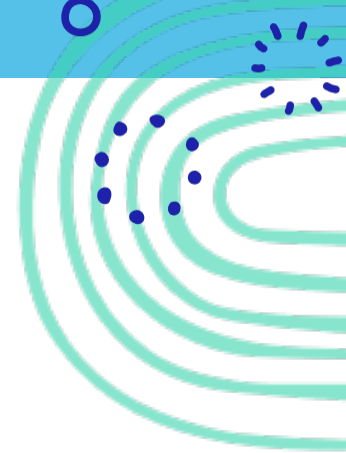
Machine learning supports predictive maintenance, anomaly detection, and classification in medical devices using data-driven models.

## Importance of Data Quality

High-quality, representative training data is crucial to avoid bias and ensure reliable AI model performance in healthcare settings.

## Model Validation and Drift

Validation techniques and monitoring model drift ensure AI systems maintain accuracy and adapt to evolving clinical environments.



# AI IN MEDICAL DEVICES AND PREDICTIVE MAINTENANCE

# AI-ENHANCED MEDICAL DEVICES AND SMART DIAGNOSTICS



## AI-Driven Device Adaptation

AI enables medical devices to autonomously adjust based on real-time patient data, improving comfort and care effectiveness.

## Enhanced Diagnostic Imaging

Deep learning algorithms improve MRI and CT scan quality, reduce time, and provide clearer diagnostic insights for clinicians.

## Smart Monitoring and Alerts

AI-powered smart alarms reduce false alerts by accurately distinguishing critical events, improving clinical response efficiency.

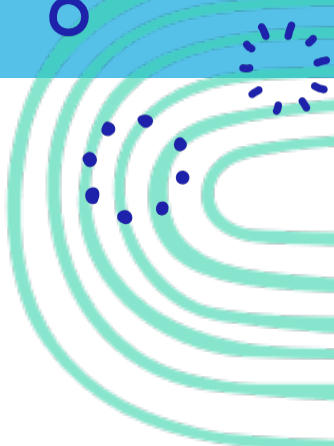
## Proactive Device Diagnostics

Embedded AI diagnostics detect device issues early, enabling proactive maintenance and enhancing patient safety and uptime.



# **CYBERSECURITY, INTEROPERABILITY, AND REGULATORY FRAMEWORKS**





# **ETHICAL CONSIDERATIONS, CLINICAL ENGINEERING ROLE, AND FUTURE TRENDS**

# FUTURE TREND:

AI can retrieve, synthesize, and contextualize information in seconds. Knowing things is no longer a durable strategy for long term relevance

. Regulatory and administrative moats that once protected many healthcare roles will increasingly erode under pressure for access, scale, and cost reduction.

Students of today and tomorrow are stuck training in an old model while a new one is rapidly evolving all around them

- METR
- OpenAI *"GPT-5.3-Codex is our first model that was instrumental in creating itself. The Codex team used early versions to debug its own training, manage its own deployment, and diagnose test results and evaluations."*

# READINESS SKILLS: AUTONOMY LEVELS

## Autonomy Level

- Levels 0–5 autonomy applied to medical devices; increasing automation with human oversight.

## MultiModal AI

- AI models combining imaging, vitals, text, telemetry for deeper contextual insights.

## Edge AI

- On-device AI enables low-latency decisions, resilience, and reduced cloud dependency

# READINESS SKILLS:

## Data Literacy

- CEs must understand datasets, bias, drift, and algorithm performance to manage AI systems

## Cybersecurity

- AI-driven anomaly detection, ML model patching, IoMT risk scoring, zero-trust integration.

## AI Validation

- Continuous model validation, performance checks post-update, governance for learning systems

## Workflow Integration

- Human factors, clinician adoption, safe rollout of semi-autonomous systems

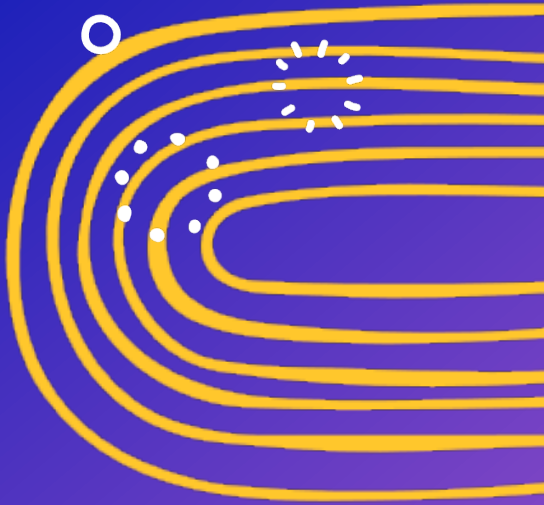
## Collaboration

- CE + IT + Security + Clinicians + Vendors = safe, effective AI adoption

# READINESS SKILLS:

## Questions to ponder in this brave new world of AI

- Where is human judgment truly indispensable?
- Where is empathy, trust, and presence non-negotiable?
- Which specialties rely on procedural skill, real-time decision-making, and accountability that can't be easily automated?
- What roles sit at the intersection of medicine, leadership, systems design, and ethics?



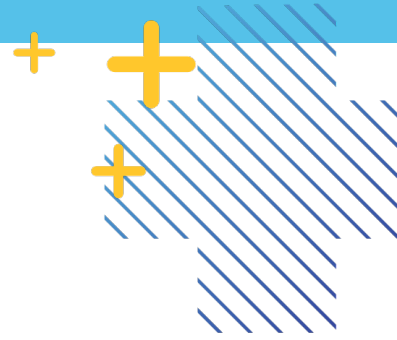
# Questions

# Panel Discussion

Moderator: Peter Dziezic



# Meet Our Panelists



**Perry Kirwan**  
Executive, Clinical Engineering  
Sutter Health



**Phil Englert**  
VP Medical Devices Security  
Health-ISAC



**Mahesh Chintakunta**  
Sr Director, Cybersecurity Ops  
RUSH



**Bill Riley**  
Sr Information Security Engineer  
Mayo Clinic



**Ernest Liu**  
Sr. Engineer  
Siemens

# “Future-ready healthcare: From Evolution to Revolution”

Are we closer to “from”  
or  
to “to” ?

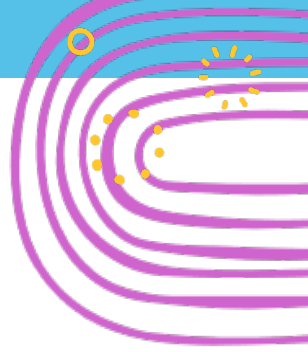




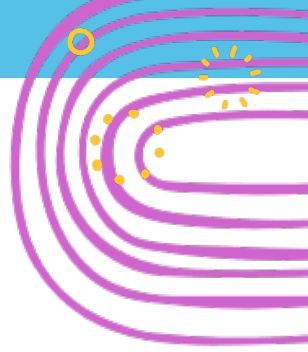
## Key Skills

Are we truly entering a healthcare technology revolution, or still evolving incrementally?

What signals define this shift?

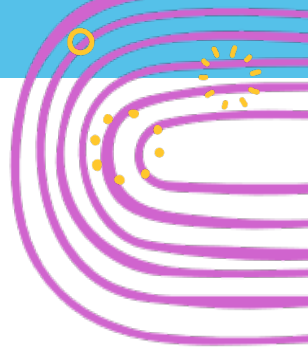


**How can CE-IT teams integrate disruptive technologies like AI and cloud-based tools into legacy environments without compromising safety or performance?**



**What does “operational readiness” look like when cyber incidents are routine and directly impact patient care?**

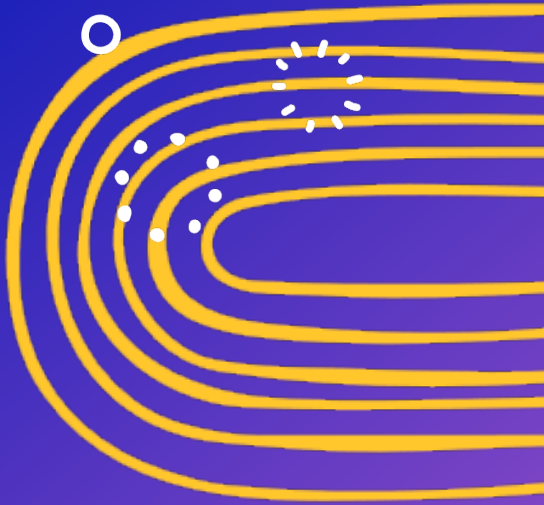
**How can CE-IT, cybersecurity, and clinical teams build a shared operational model for rapid response during cyber-physical incidents?**



**What does “operational readiness” look like when cyber incidents are routine and directly impact patient care?**

**How can CE-IT, cybersecurity, and clinical teams build a shared operational model for rapid response during cyber-physical incidents?**

**As AI becomes embedded in diagnostics and workflows, what new responsibilities must HTM and IT teams take on to ensure clinical safety and accountability?**



# Questions

# Thank you to our CE-IT Symposium task force team:



Juuso Leinonen



Mike Powers



Peter Dzedzic



Keith Whitby



Suly Chi



Priyanka Shah



Chris Nowak



Priyanka Sollinger



Future-Ready Healthcare  
From Evolution to Revolution

Thank you for  
attending!

