2023 ACCE CE-IT Symposium

Securing IoMT Proactively

Collaboration Between Information Technology and Clinical Engineering Profession

ACCE would like to thank our co-sponsors

Platinum Sponsor

Gold Sponsor

Turning the Tide: Developing Cyber Safety Partnerships with Clinicians

Dr. Christian Dameff MD, MS, FACEP

Assistant Professor, UC San Diego

UC San Diego

UC San Diego

About the keynote speaker

Dr. Christian Dameff is an assistant professor of Emergency Medicine, Biomedical Informatics, and Computer Science (affiliate) at the University of California San Diego. At UCSD Health he was hired as the nation's first Medical Director of Cyber Security.

Dr. Dameff is also a hacker and security researcher interested in the intersection of healthcare, patient safety, and cybersecurity. He has spoken at some of the world's most prominent Cyber Security forums including DEFCON, RSA, Blackhat, and BSides, and is one of the cofounders of the CyberMed Summit, a novel multidisciplinary conference with emphasis on medical device and infrastructure cybersecurity. Published cybersecurity topics include hacking 911 systems, HL7 messaging vulnerabilities, and malware.

Session Description

1. Introduction
2. Group therapy
3. Barriers clinician pose to good security practices
4. Tips for success
5. Alignment: the big picture
6. Questions

Emergency Medicine

“SECURE” Telemedicine

zoom

Hacker

WIRED How Hackers Could Mess With 911 Systems and Put You at Risk SUBSCRIBE

BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION

KIM ZETTER SECURITY 08.21.14 6:30 AM

HOW HACKERS COULD MESS WITH 911 SYSTEMS AND PUT YOU AT RISK

DARK Daily
Serving Clinical Labs & Pathology Groups

University of California San Diego Researchers Demonstrates How Easily Medical Laboratory Systems and Devices Can Be Compromised, Putting Patient Lives at Risk

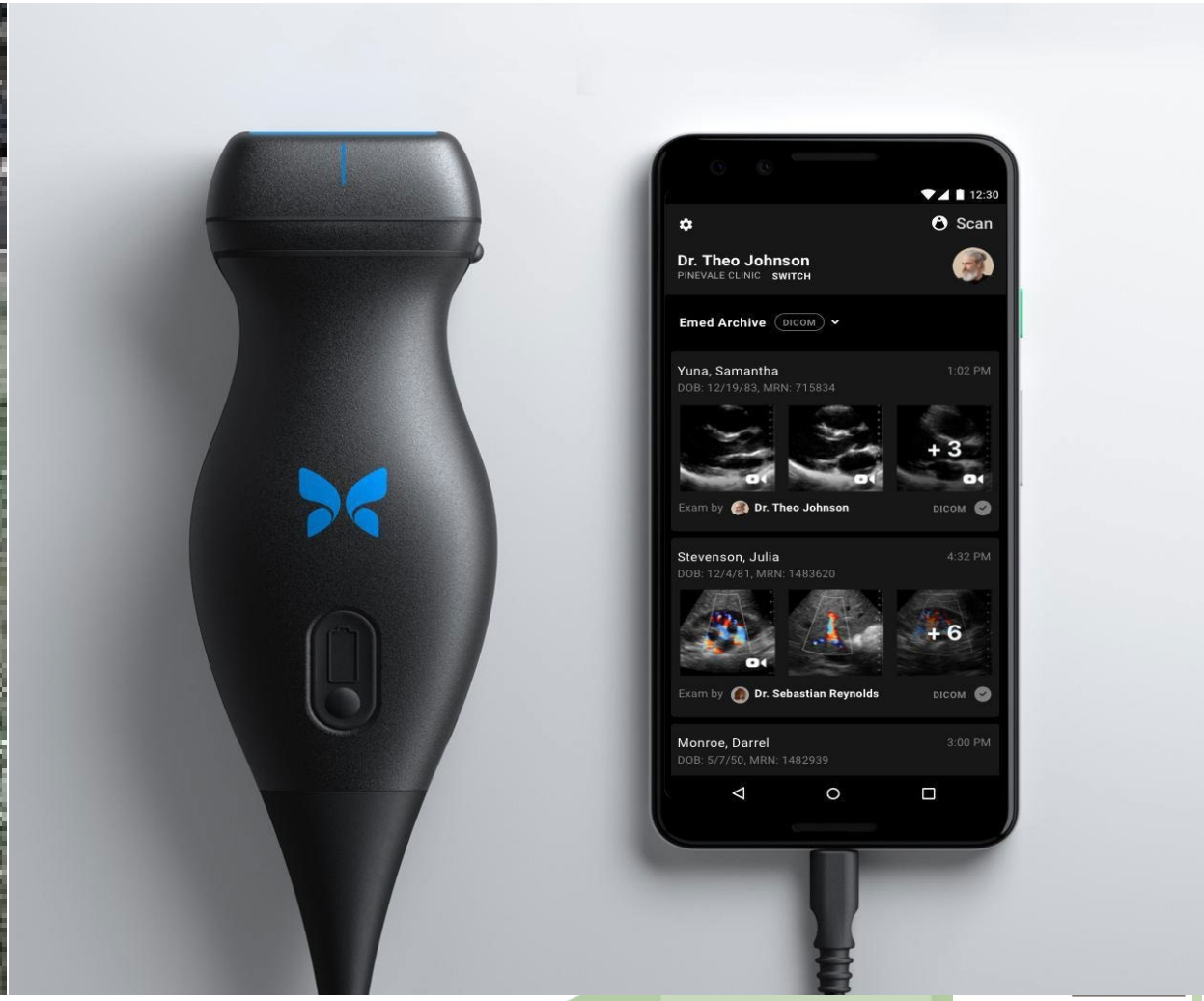
Mar 8, 2019 | Laboratory Management and Operations, Laboratory News, Laboratory Operations, Laboratory Pathology, Management & Operations

Researchers stress the importance of preparing hospital and clinical laboratory information systems before a 'major failure' occurs

Medical laboratory information systems (LIS) and similar devices are vulnerable to hacking, according to physicians and computer scientists from the University of California San Diego (UCSD) and the University of California Davis (UCD). They recently completed a study that exposed the vulnerabilities of these systems and revealed how clinical laboratory test results can be manipulated and exploited to put patient lives at risk.

Group Therapy Time

Group Therapy

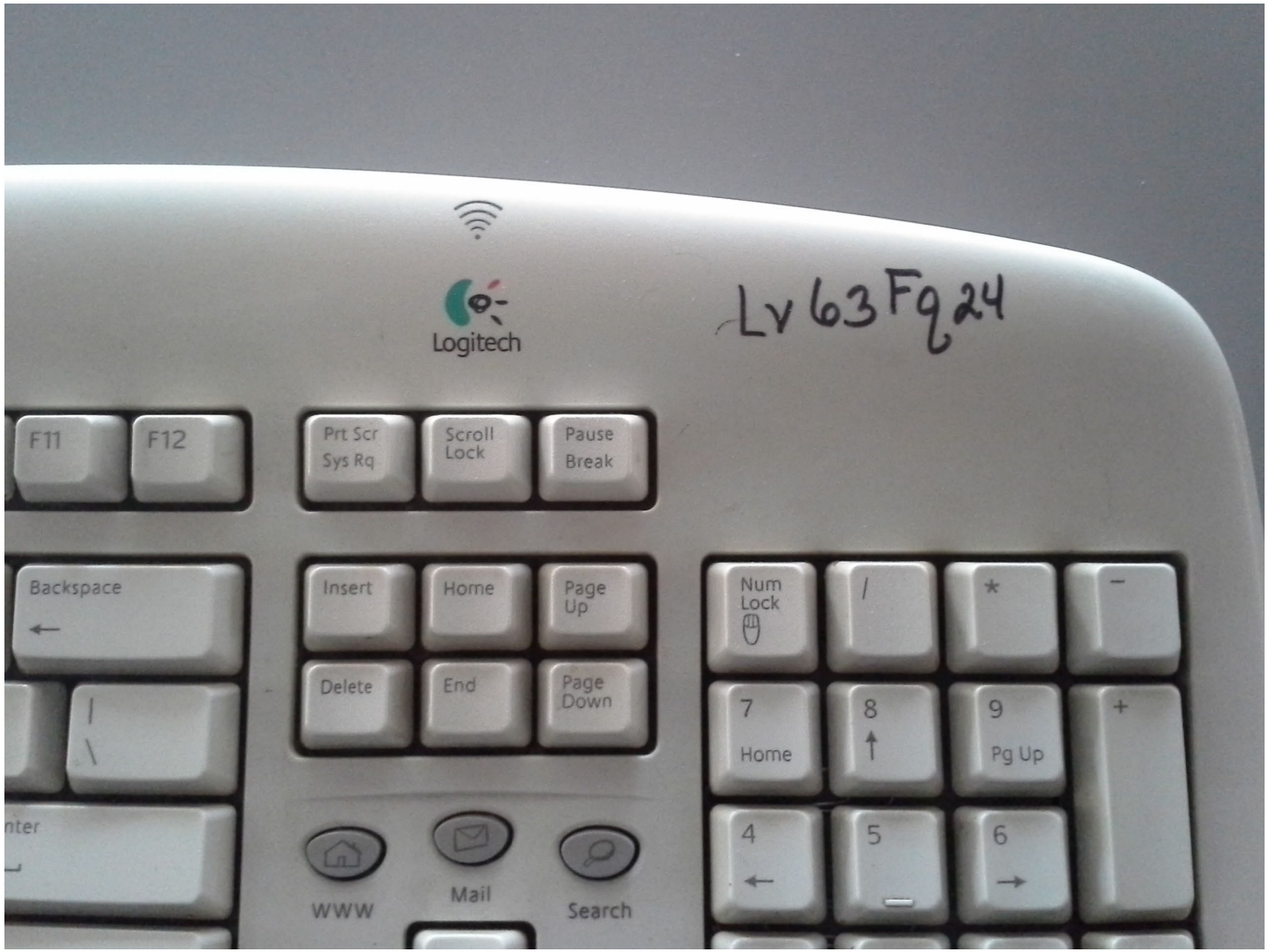


Group Therapy

“Make it work and don’t bother me with a password.”

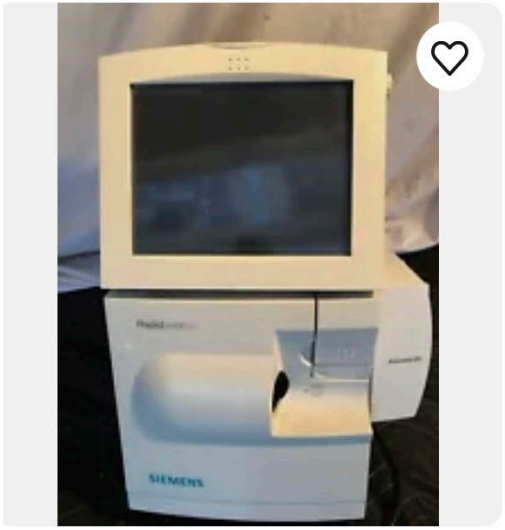
Pitfall: Procurement

Pitfall: Deployment



Pitfall: Clinical Use

Pitfall: Decommissioning



Siemens Rapidpoint 405 Blood Gas Analyzer

Pre-Owned

$9.95

or Best Offer

+$182.75 shipping

7 watchers

akbuy.shop (236) 100%

Converting Clinicians

Tip: Show Clinical Impact

Converting Clinicians

Converting Clinicians

Converting Clinicians

https://www.youtube.com/watch?v=OpyYLJOLwpA&t=38s

Converting Clinicians

PubMed.gov
US National Library of Medicine
National Institutes of Health

PubMed

Advanced

Format: Abstract

Send to

J Emerg Med. 2018 Dec 12. pii: S0736-4679(18)31055-2. doi: 10.1016/j.jemermed.2018.10.029. [Epub ahead of print]

Clinical Cybersecurity Training Through Novel High-Fidelity Simulations.

Dameff CJ[1], Selzer JA[2], Fisher J[2], Killeen JP[1], Tully JL[3].

Author information

Abstract

BACKGROUND: Cybersecurity risks in health care systems have traditionally been measured in data breaches of protected health information, but compromised medical devices and critical medical infrastructure present risks of disruptions to patient care. The ubiquitous prevalence of connected medical devices and systems may be associated with an increase in these risks.

OBJECTIVE: This article details the development and execution of three novel high-fidelity clinical simulations designed to teach clinicians to recognize, treat, and prevent patient harm from vulnerable medical devices.

METHODS: Clinical simulations were developed that incorporated patient-care scenarios featuring hacked medical devices based on previously researched security vulnerabilities.

RESULTS: Clinicians did not recognize the etiology of simulated patient pathology as being the result of a compromised device.

CONCLUSIONS: Simulation can be a useful tool in educating clinicians in this new, critically important patient-safety space.

Copyright © 2018 Elsevier Inc. All rights reserved.

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Tip: Identify the Willing

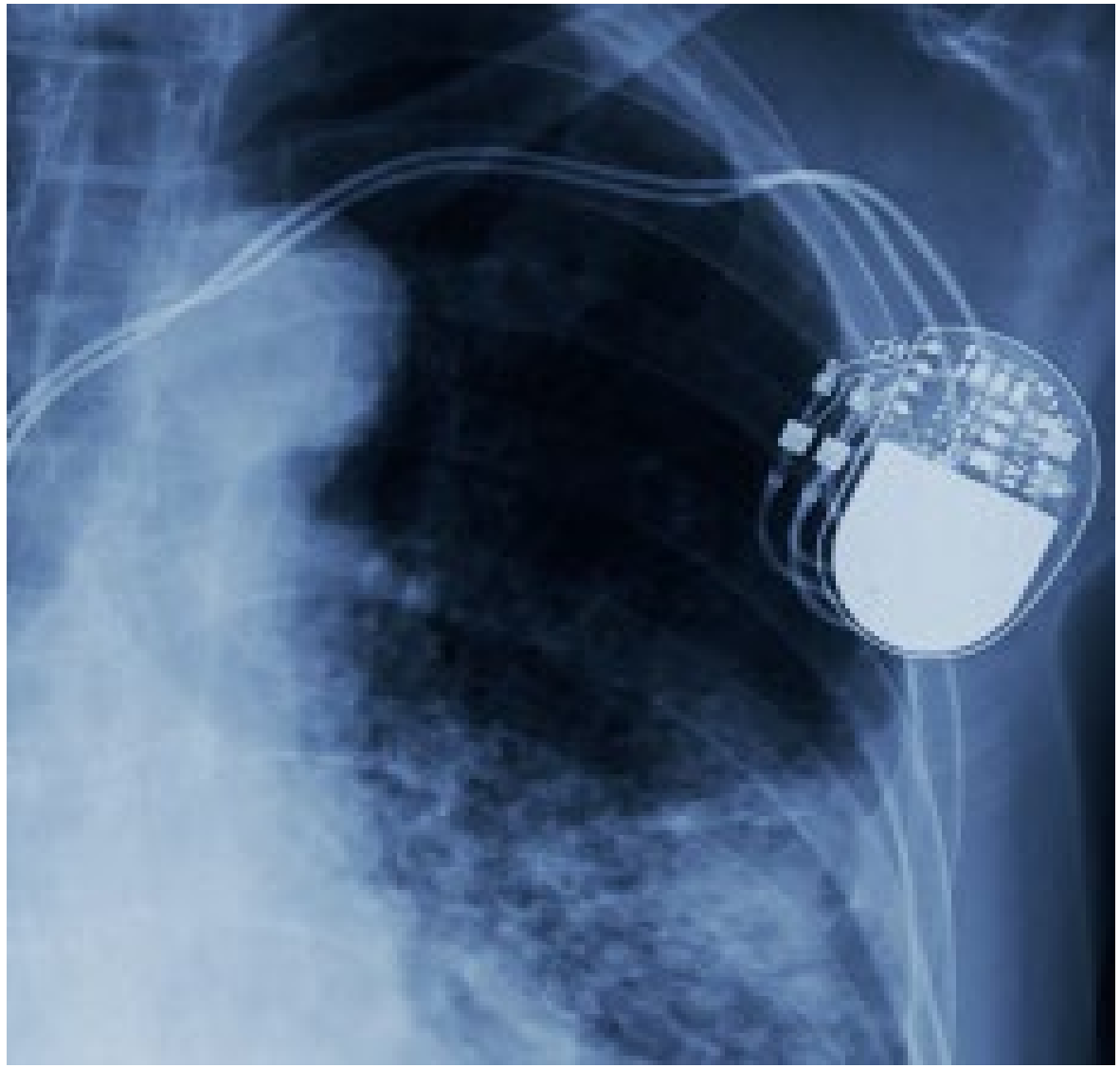
Tip: Talk About Big Risks

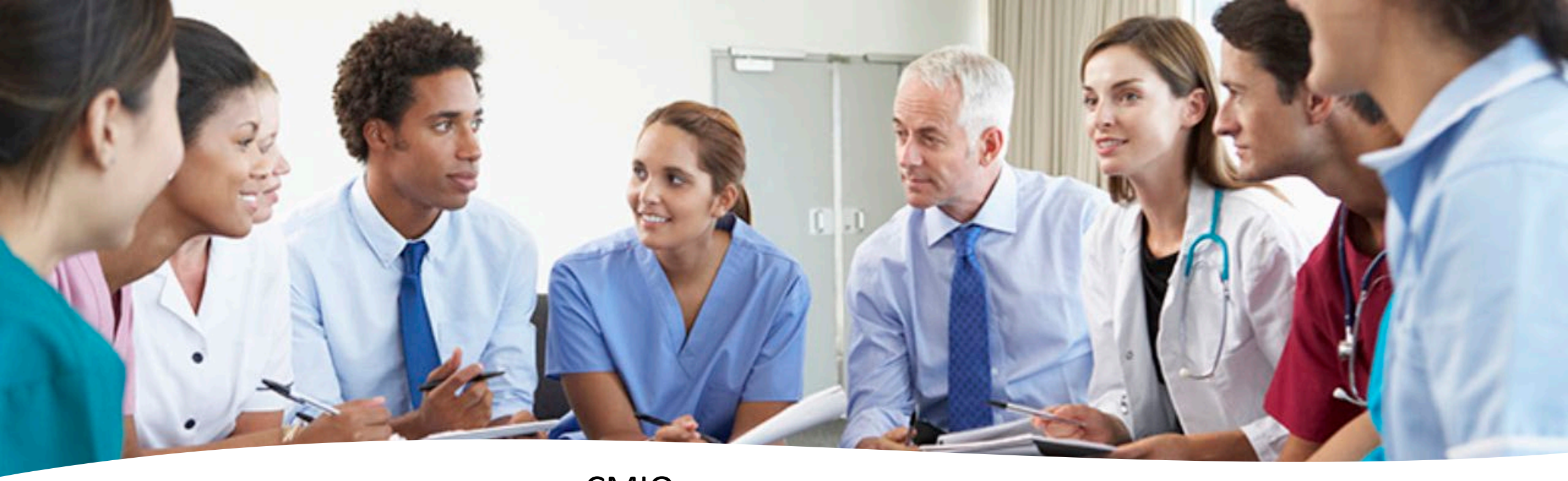
The San Diego Union-Tribune

Subscribe Now
$4/4 weeks

Scripps enters fourth week of ransomware attack

Tip: Specialty Matters





Tip: Build a Team

- CMIO
- CISO
- Clinical engineering leadership
- Emergency Managers
- Residents, fellows, nurses, etc.
- “Medical Device Cybersecurity Committee”

The Big Picture: Alignment

- Clinical Engineering
- Information Services
- Clinicians

TechTarget | HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home News Features Interviews

HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches | Disaster

How Sen. Warner Aims to Mitigate Healthcare Cybersecurity Risks Through Legislation

Senator Mark Warner spoke with HealthITSecurity about the healthcare cybersecurity challenges discussed in his recent policy options paper and how he plans to address them.

As hospitals see increased cybersecurity scrutiny, the true state of medical device security will come to light.

Start working now.

Questions?