Northeastern University

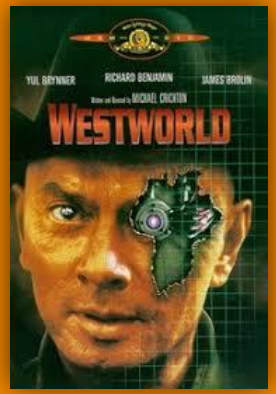
Medical Device Cybersecurity – Week 14

04/07/2026: Closing Topics

Axel Wirth | Chief Security Strategist | Medcrypt
axel@medcrypt.com

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- HDO Perspective
- The Future is Near – What's Next?
- Regulatory Topics Roundup



"There's a clear pattern here which suggests an analogy to an infectious disease process, spreading from one area to the next. …
I must confess, I find it difficult to believe in a disease of machinery."

From the Movie Westworld (1973)

The Secure Development Lifecycle (SDLC) Context

- General Premarket activities
- Postmarket begins after regulatory approval:
  - Release for sale
  - Manufacturing transfer
- Applies to all new products, versions, and updates & patches

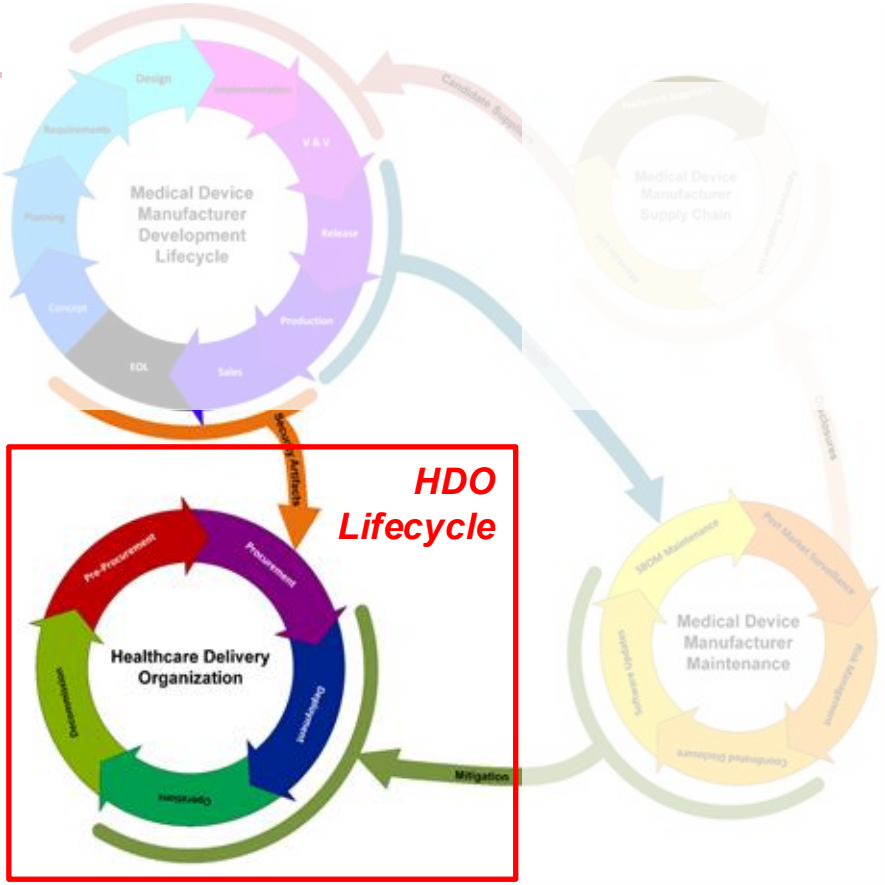
- Supply Chain Management
- Vulnerability Monitoring
- Contract and relationship management

HDO Perspective:
- Procurement
- Onboarding
- Maintenance
- Decommissioning

- Patches and Updates
- Documentation
- Risk Communication
  - Vulnerabilities
  - Threats
  - EOL / EOS

The Secure Development Lifecycle (SDLC) Context

- General Premarket activities
- Postmarket begins after regulatory approval:
  - Release for sale
  - Manufacturing transfer
- Applies to all new products, versions, and updates & patches



HDO Perspective:
- Procurement
- Onboarding
- Maintenance
- Decommissioning

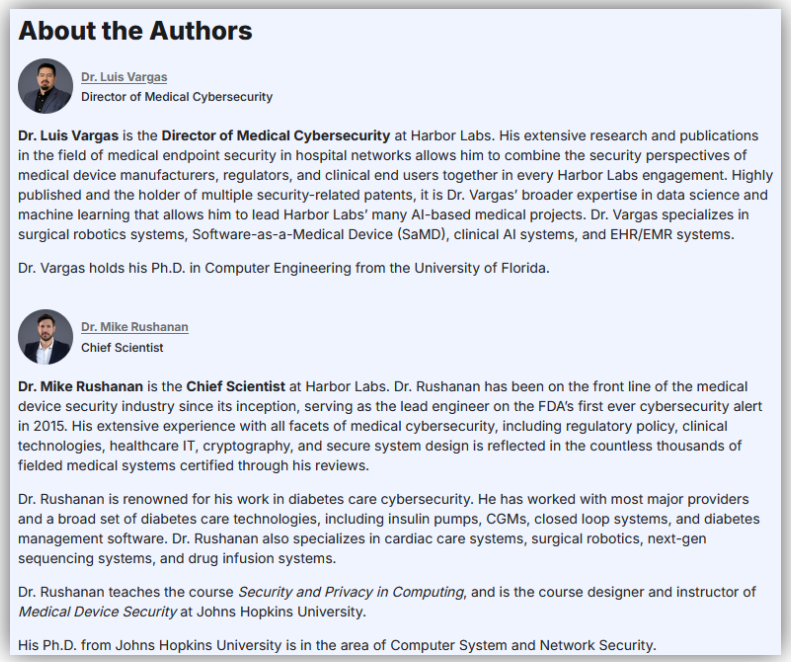
- Supply Chain Management
- Vulnerability Monitoring
- Contract and relationship management

- Patches and Updates
- Documentation
- Risk Communication
  - Vulnerabilities
  - Threats
  - EOL / EOS

Sometimes Someone Else does your Work for you

“A Candid Perspective on Hospital IT Teams and Medical Device Cybersecurity” (Harbor Labs)

- Hospitals Start from a Position of Distrust
- IT Security Often Enters the Process Late
- A Good MDS2 Makes a Huge Difference
- Hospitals Rarely Test Devices Themselves
- A Three-Way Disconnect Exists
- Vendors Sometimes Shift Risk to Hospitals
- Incident Response Capabilities Are Often Limited
- SBOMs Exist — But Are Rarely Used



About the Authors

Dr. Luis Vargas
Director of Medical Cybersecurity

Dr. Luis Vargas is the **Director of Medical Cybersecurity** at Harbor Labs. His extensive research and publications in the field of medical endpoint security in hospital networks allows him to combine the security perspectives of medical device manufacturers, regulators, and clinical end users together in every Harbor Labs engagement. Highly published and the holder of multiple security-related patents, it is Dr. Vargas' broader expertise in data science and machine learning that allows him to lead Harbor Labs' many AI-based medical projects. Dr. Vargas specializes in surgical robotics systems, Software-as-a-Medical Device (SaMD), clinical AI systems, and EHR/EMR systems.

Dr. Vargas holds his Ph.D. in Computer Engineering from the University of Florida.

Dr. Mike Rushanan
Chief Scientist

Dr. Mike Rushanan is the **Chief Scientist** at Harbor Labs. Dr. Rushanan has been on the front line of the medical device security industry since its inception, serving as the lead engineer on the FDA's first ever cybersecurity alert in 2015. His extensive experience with all facets of medical cybersecurity, including regulatory policy, clinical technologies, healthcare IT, cryptography, and secure system design is reflected in the countless thousands of fielded medical systems certified through his reviews.

Dr. Rushanan is renowned for his work in diabetes care cybersecurity. He has worked with most major providers and a broad set of diabetes care technologies, including insulin pumps, CGMs, closed loop systems, and diabetes management software. Dr. Rushanan also specializes in cardiac care systems, surgical robotics, next-gen sequencing systems, and drug infusion systems.

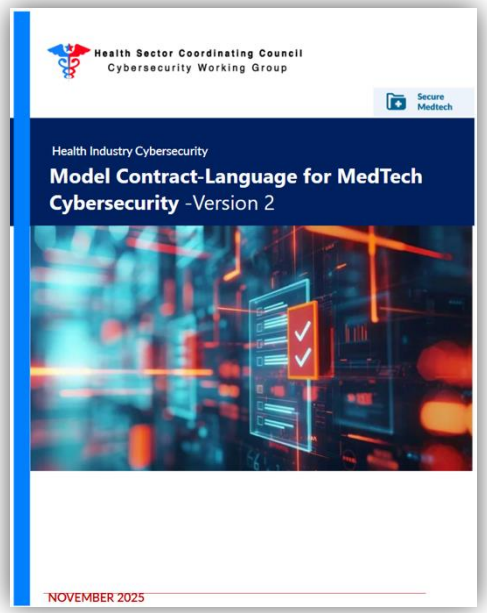
Dr. Rushanan teaches the course *Security and Privacy in Computing*, and is the course designer and instructor of *Medical Device Security* at Johns Hopkins University.

His Ph.D. from Johns Hopkins University is in the area of Computer System and Network Security.

https://harborlabs.com/medical-device-cybersecurity-hospital-it-perspective/

How Hospitals Can (Need to) Address Cybersecurity
Example - Procurement

- Manufacturer Maturity
  - Standards Alignment
  - Secure Development Lifecycle
  - Maintenance & Transparency
- Product Maturity
  - Network Security
  - Physical Security
  - Malware Protection & Intrusion Detection
  - Audit & Logging
  - Encryption
  - Access Management
  - Secure Updating & Patching
  - Risk & Attack Surface Reduction
- Performance
  - Vulnerability & Incident Management
  - Customer Support



https://healthsectorcouncil.org/wp-content/uploads/2025/11/MC2v2.pdf

How Hospitals Can (Need to) Address Cybersecurity
Example – Security Documentation

Security-relevant documents – user and FDA expectation:

- User = operator / maintainer (clinical / technical) but also patients, …
- Part of “cybersecurity transparency”
- Documentation is used to a) assess MDM maturity; b) securely operate and maintain devices

Examples:

- Manufacturer Disclosure Statement for Medial Device Security (MDS^2)
- Security controls and controls maintenance (e.g., anti-malware)
- List of ports and interfaces
- Supporting infrastructure
- Supporting diagrams
- SBOM
- SW/FW update notifications, distribution, and instructions
- Device incident detection and response behavior
- Security event detection and logging; forensic evidence capture
- Protective features (e.g., backup, retention and recovery of device configuration)
- Secure configuration and user-configurable security features
- Expected EOL/EOS
- Decommissioning features

How Hospitals Can (Need to) Address Cybersecurity

Example – Managing Security

Inventory Visibility:

- Know what's on your network
- Know security properties
- Understand integration & dependencies
- Identify risk & plan a path forward

Today's Inventory Reality:

- Legacy & disparate inventory systems (CMMS, CMBD)
- Many systems not security-aware
- Devices may not be network scannable or discoverable

Network Best Practices:

- Segment based on risk, functional needs, redundancies, etc.
- Monitor network traffic
- Use secure / encrypted protocols
- Secure remote access

Today's Network Reality:

- Flat or only rudimentary segmentation
- Legacy devices may force everything to the lowest common denominator
- Encrypted protocols (DICOM, HL7) not utilized … for a variety of reasons

Cybersecurity Technologies – Passive Network Monitoring

SPAN/TAP connection

External sources:
- Recalls and advisories
- Vulnerability disclosure
- Manufacturer security data (e.g., MDS2)
- Community-derived

PNM Solution

Integration with:
- Asset management (CMMS/CMDB)
- Risk tools
- IT Security tools

Provides:
- Pre-procurement assessment
- Supply chain risk mgmt.
- Recall management
- Security best practices
- Traffic analysis
- Behavior baseline
- Security event detection
- Usage & network statistics
- Vulnerability identification
- Risk remediation prioritization

How Hospitals Can (Need to) Address Cybersecurity

- Procurement and replacement planning
- Staffing, Training, and Budgets
- Vendor relationship
- Security Transparency
- Inventory quality
- Vulnerability management / risk reduction
- End-of-Life Management
- Secure decommissioning
- Network segmentation
- Supplemental security (from firewalls to network-based detection)

Just in from Texas

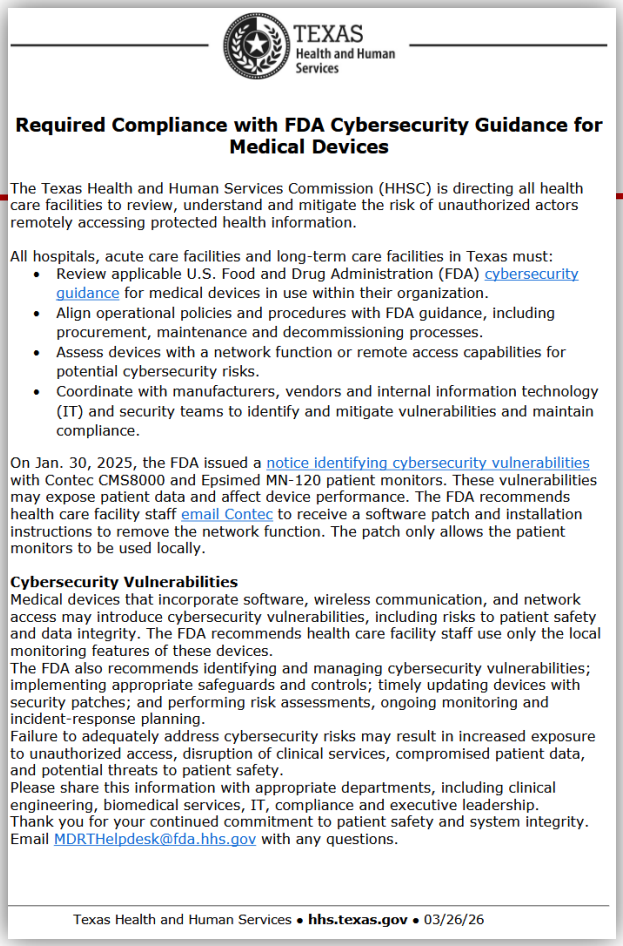
All hospitals, acute care facilities and long-term care facilities in Texas must (summarized):

- Review FDA cybersecurity guidance for medical devices
- Align operational policies and procedures with FDA guidance, including procurement, maintenance and decommissioning processes.
- Assess devices for potential cybersecurity risks.
- Identify and mitigate vulnerabilities and maintain compliance.

Directed by Texas HHSC on 3/26/26

Following executive order by Governor Greg Abbott addressing China-made devices (3/9/26)

But – unclear consequences of non-compliance



TEXAS Health and Human Services

Required Compliance with FDA Cybersecurity Guidance for Medical Devices

The Texas Health and Human Services Commission (HHSC) is directing all health care facilities to review, understand and mitigate the risk of unauthorized actors remotely accessing protected health information.

All hospitals, acute care facilities and long-term care facilities in Texas must:

- Review applicable U.S. Food and Drug Administration (FDA) cybersecurity guidance for medical devices in use within their organization.
- Align operational policies and procedures with FDA guidance, including procurement, maintenance and decommissioning processes.
- Assess devices with a network function or remote access capabilities for potential cybersecurity risks.
- Coordinate with manufacturers, vendors and internal information technology (IT) and security teams to identify and mitigate vulnerabilities and maintain compliance.

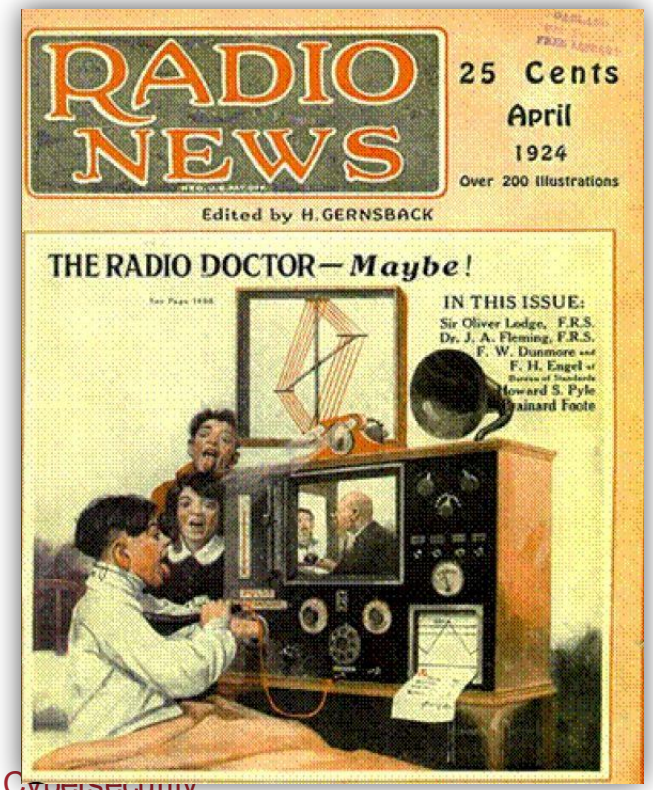
On Jan. 30, 2025, the FDA issued a notice identifying cybersecurity vulnerabilities with Contec CMS8000 and Epsimed MN-120 patient monitors. These vulnerabilities may expose patient data and affect device performance. The FDA recommends health care facility staff email Contec to receive a software patch and installation instructions to remove the network function. The patch only allows the patient monitors to be used locally.

Cybersecurity Vulnerabilities
Medical devices that incorporate software, wireless communication, and network access may introduce cybersecurity vulnerabilities, including risks to patient safety and data integrity. The FDA recommends health care facility staff use only the local monitoring features of these devices.
The FDA also recommends identifying and managing cybersecurity vulnerabilities; implementing appropriate safeguards and controls; timely updating devices with security patches; and performing risk assessments, ongoing monitoring and incident-response planning.
Failure to adequately address cybersecurity risks may result in increased exposure to unauthorized access, disruption of clinical services, compromised patient data, and potential threats to patient safety.
Please share this information with appropriate departments, including clinical engineering, biomedical services, IT, compliance and executive leadership.
Thank you for your continued commitment to patient safety and system integrity.
Email MDRTHelpdesk@fda.hhs.gov with any questions.

Texas Health and Human Services • **hhs.texas.gov** • 03/26/26

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

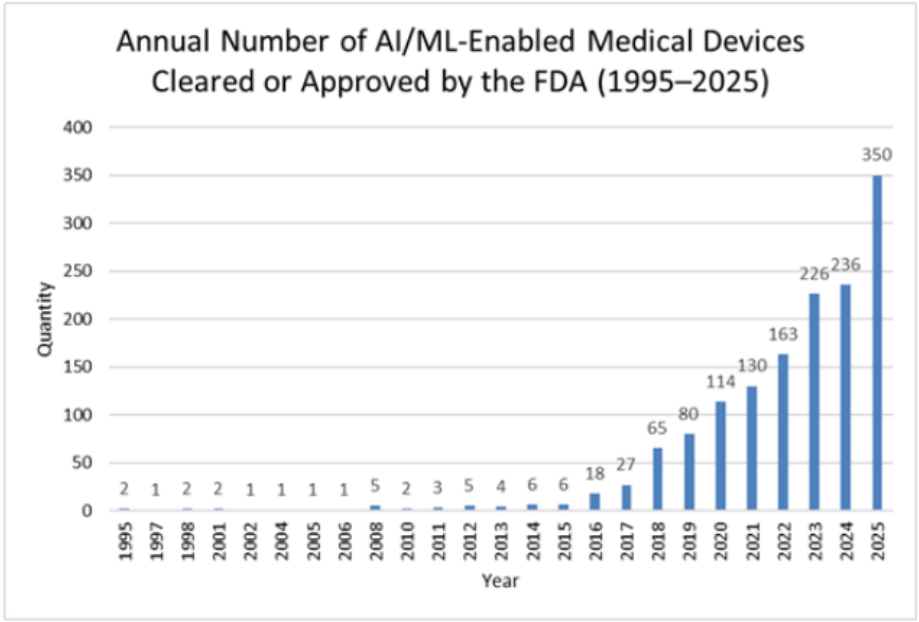
- HDO Perspective
- The Future is Near – What's Next?
- Regulatory Topics Roundup



The AI Trifecta

Secure AI-Systems	AI–based Security	AI as Attack Tool
• Comply with privacy and AI-specific laws • Protect you AI intellectual property • Protect AI systems and data from manipulation & attack • Protect AI infrastructure from learning data to deployment • Prevent “well-intended” compromises (shadow AI, data leakage)	• Discover vulnerabilities • Support threat intelligence • Analyze complex security events across control points • Monitor event logs and support risk decisions • Orchestrate response • Coordination and communication	• Corrupt or compromise AI systems (e.g., model poisoning) • Discover vulnerabilities and misconfigurrations • Create malware and exploits at speed • Craft highly targeted attacks • Realistic social engineering and disinformation campaigns • Lower entry barrier • Orchestrate attacks

AI-based Medical Devices Becoming Mainstream



Source: FDA, 2026

For a complete listing see FDA website here: https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-enabled-medical-devices

https://www.linkedin.com/pulse/ai-enabled-medical-devices-fda-analyzing-30-years-19952025-rivel-uiqee/

AI as a Cyber Threat

Example: Use of AI to Manipulate CT Images

- Security researchers used Machine Learning algorithm to introduce / remove evidence of cancer
- Radiologists and an AI Tool evaluated the images:
  - Radiologists were fooled 99% of the time for injection, and 94% of the time for removal
  - The AI system was fooled 100% of the time (but – this was 2019!)

https://securityaffairs.co/wordpress/83412/hacking/computer-tomography-scans-hack.html

Hackers can add, remove cancer and other illnesses from Computer Tomography scans

April 5, 2019 By Pierluigi Paganini

Researchers demonstrated that hackers can modify 3D Computer Tomography scans to add or remove evidence of a serious illness, including cancers.

A group of researchers from the Ben-Gurion University and the Soroka University Medical Center, Beer-Sheva, in Israel, have demonstrated that hackers can modify 3D medical scans to the result of a clinical examination.

Attackers can add or remove evidence of various illnesses, including aneurysms, heart disease, blood clots, infections, arthritis, cartilage problems, torn ligaments, and tumors in the brain, heart or spine.

The experts developed proof-of-concept (PoC) malware that uses a machine learning technique known as generative adversarial network (GAN) to alter 3D images generated during a Computer Tomography (CT) scan. Scans are sent to picture archiving and communication systems (PACS) that store them. The format used to transmit and store the images is DICOM. GE Healthcare, Fujifilm, Philips, and RamSoft are main vendors of PACS systems.

PACS and DICOM servers are often left exposed to the Internet, the experts found roughly 2,700 servers exposed online using the Shodan search engine.

The experts also discovered that medical imagery data are transmitted without encryption, an attacker can potentially run man-in-the-middle (MitM) attacks to manipulate them.

The experts conducted a penetration test in a radiology department of a hospital. In a test scenario, they connected a small MitM device between the CT scanner's workstation and the PACS network that allowed them to intercept traffic from the CT scanner. The researchers developed an attack framework dubbed CT-GAN to manipulate the images via the GAN technique.

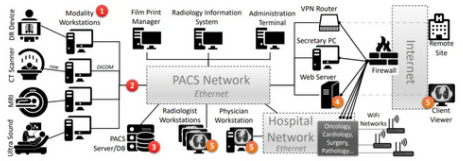
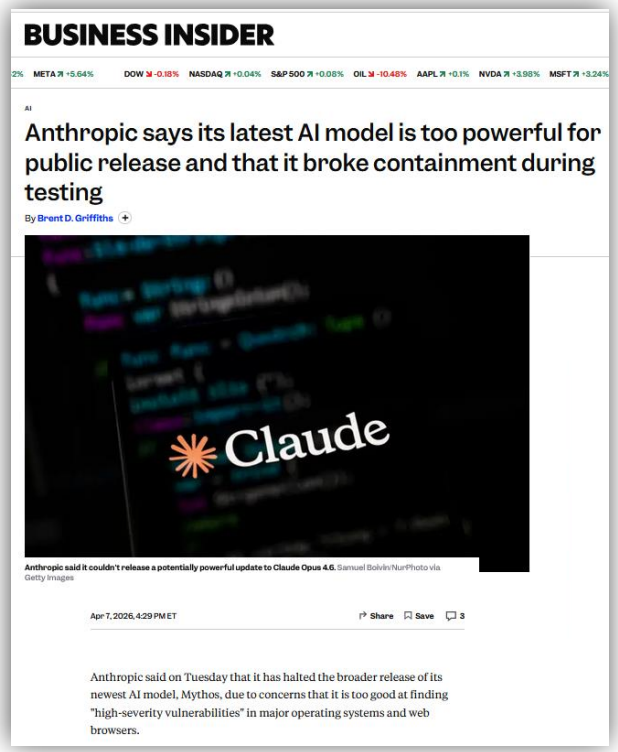


Figure 3: A network overview a PACS in a hospital. 1-3: points where an attacker can tamper with all scans. 4-5: points where an attacker can tamper with a subset of scans.

The Future is Here!



BUSINESS INSIDER

2% META +5.64% DOW -0.18% NASDAQ +0.04% S&P 500 +0.08% OIL -10.48% AAPL +0.1% NVDA +3.98% MSFT +3.24%

AI

Anthropic says its latest AI model is too powerful for public release and that it broke containment during testing

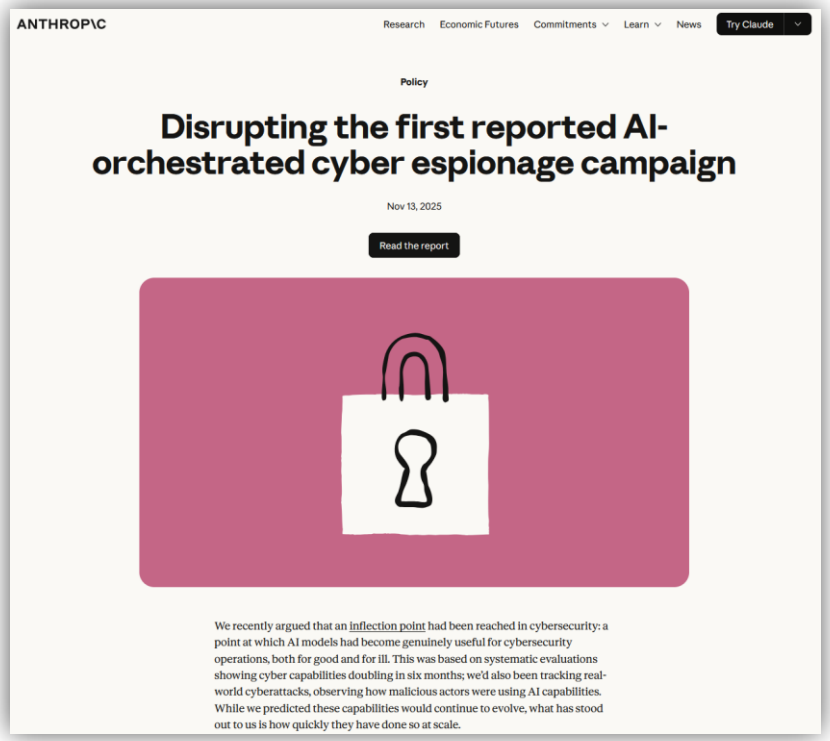
By Brent D. Griffiths

Anthropic said it couldn't release a potentially powerful update to Claude Opus 4.6. Samuel Boivin/NurPhoto via Getty Images

Apr 7, 2026, 4:29 PM ET Share Save 3

Anthropic said on Tuesday that it has halted the broader release of its newest AI model, Mythos, due to concerns that it is too good at finding "high-severity vulnerabilities" in major operating systems and web browsers.

https://www.businessinsider.com/anthropic-mythos-latest-ai-model-too-powerful-to-be-released-2026-4



ANTHROP\C

Research Economic Futures Commitments Learn News Try Claude

Policy

Disrupting the first reported AI-orchestrated cyber espionage campaign

Nov 13, 2025

Read the report

We recently argued that an inflection point had been reached in cybersecurity: a point at which AI models had become genuinely useful for cybersecurity operations, both for good and for ill. This was based on systematic evaluations showing cyber capabilities doubling in six months; we'd also been tracking real-world cyberattacks, observing how malicious actors were using AI capabilities. While we predicted these capabilities would continue to evolve, what has stood out to us is how quickly they have done so at scale.

https://www.anthropic.com/news/disrupting-AI-espionage

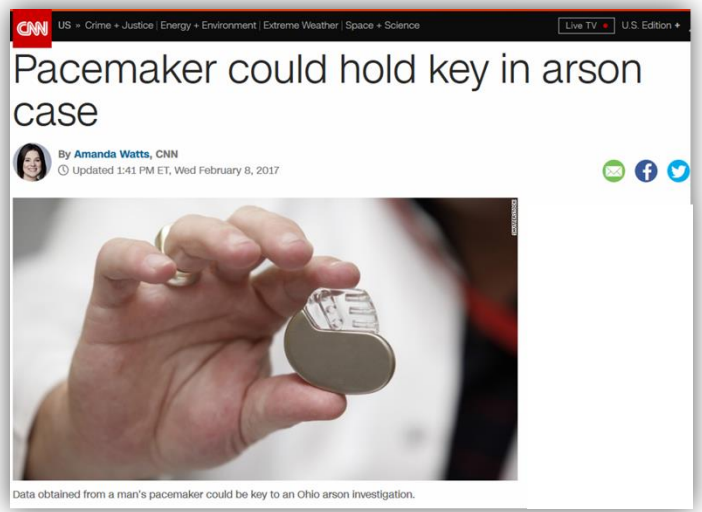
Cybersecurity Future Gazing - Telehealth

Healthcare Use Cases:

- Patient / provider communication
- Health & Wellness
- Medication adherence
- Home Care / Hospital at Home
- Remote monitoring

Security & Privacy Challenges:

- Health data on a consumer device / network
- Mixing trusted & non-trusted apps
- Device loss or theft
- Defining the HIPAA boundary
- Mixing of disparate data – health, social media, geolocation, etc.
- Unintended uses of data, e.g., law enforcement



Cybersecurity Future Gazing - Technology

Increasing Supply Chain Attacks:

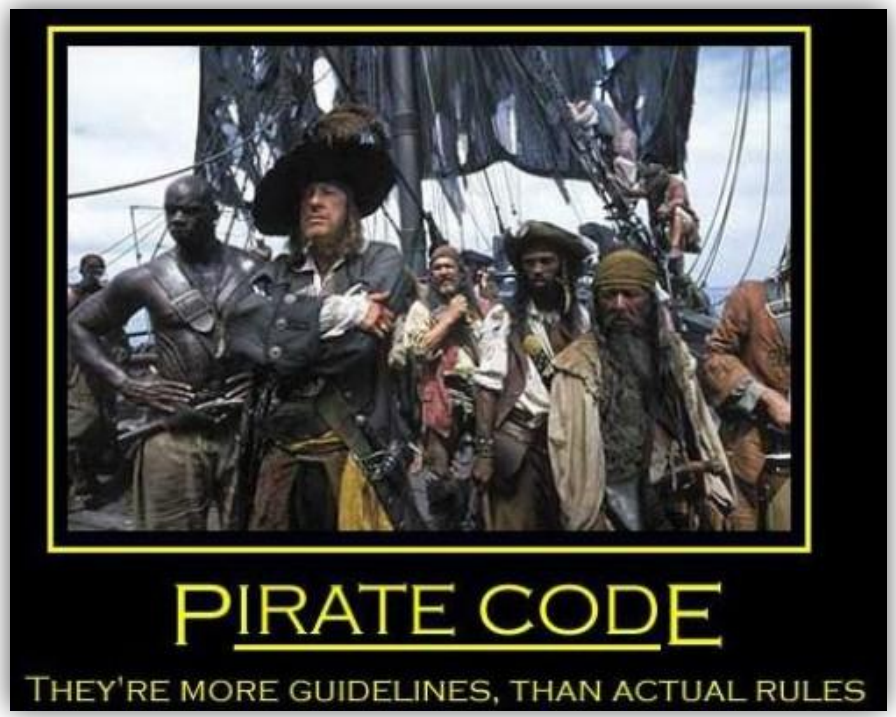
- Deliver payload (malware) via trusted 3rd party software (e.g., NotPetya):
  - Difficult to identify: Trusted domain, digitally signed, trusted update process, …
  - Benefits: Rapid distribution within a targeted industry or region
  - Circumvent traditional security controls, access with elevates privileges
- Potential to infect and utilize hardware supply chain in the future:
  - Such attack would be highly sophisticated and difficult to detect
  - Resistant to malware removal, reboot, reformatting, or reinstallation

Data-in-Transit Attacks:

- Gain access to routers and other network infrastructure:
  - Steal credentials, account, or other confidential information
  - Deliver compromised web page to capture confidential information (“formjacking”)
  - Intercept and manipulate data between sender and recipient – man-in-the middle attacks at scale

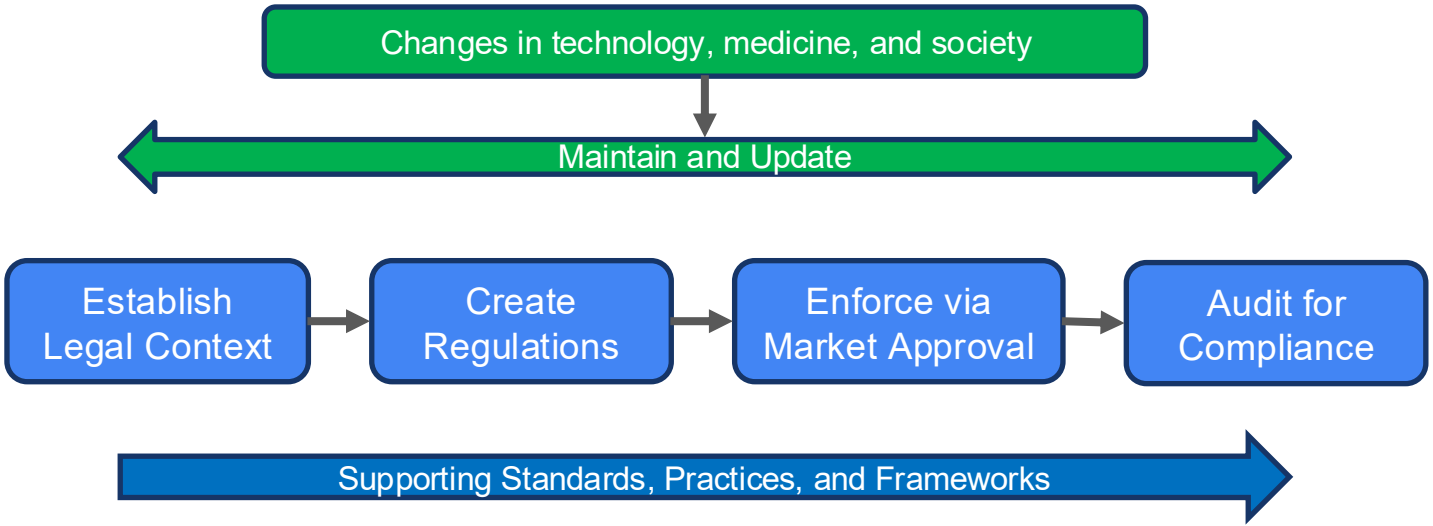
Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- HDO Perspective
- The Future is Near – What's Next?
- Regulatory Topics Roundup



Regulatory Concepts

Essentially Similar across the Globe but Implementation Details Vary



Regulatory Concepts

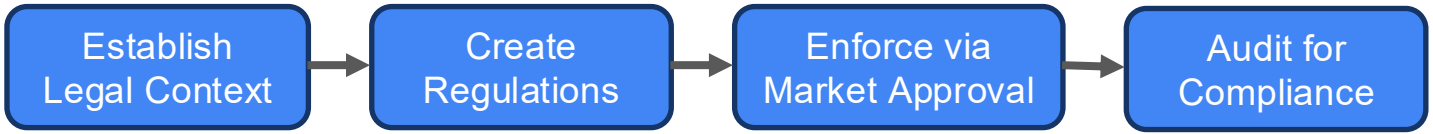
Example: US FDA

2023 FD&C Act gave FDA legal mandate and authority on cybersecurity (prior to that cyber-security as an extension of safety

FDA cybersecurity pre- and postmarket guidances; AI, …

Based on manufacturer documentation; rejections for cybersecurity reasons now common

QMSR-based audits now include cybersecurity



Published list of recognized consensus standards
https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfstandards/search.cfm

Regulatory Concepts

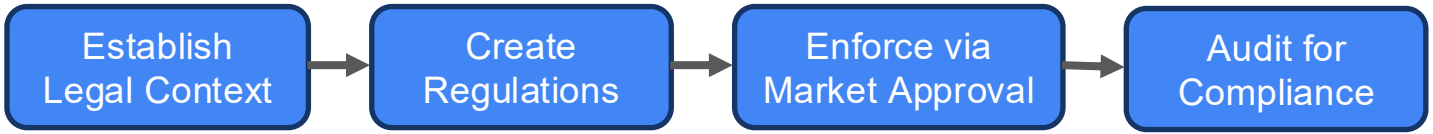
Example: EU MDR / IVDR

Per MDR/IVDR Annex I. Establishes concepts such as lifecycle management, secure by design and "state of the art" security

MDCG 2019-16 as "cybersecurity interpretation" and reference to standards

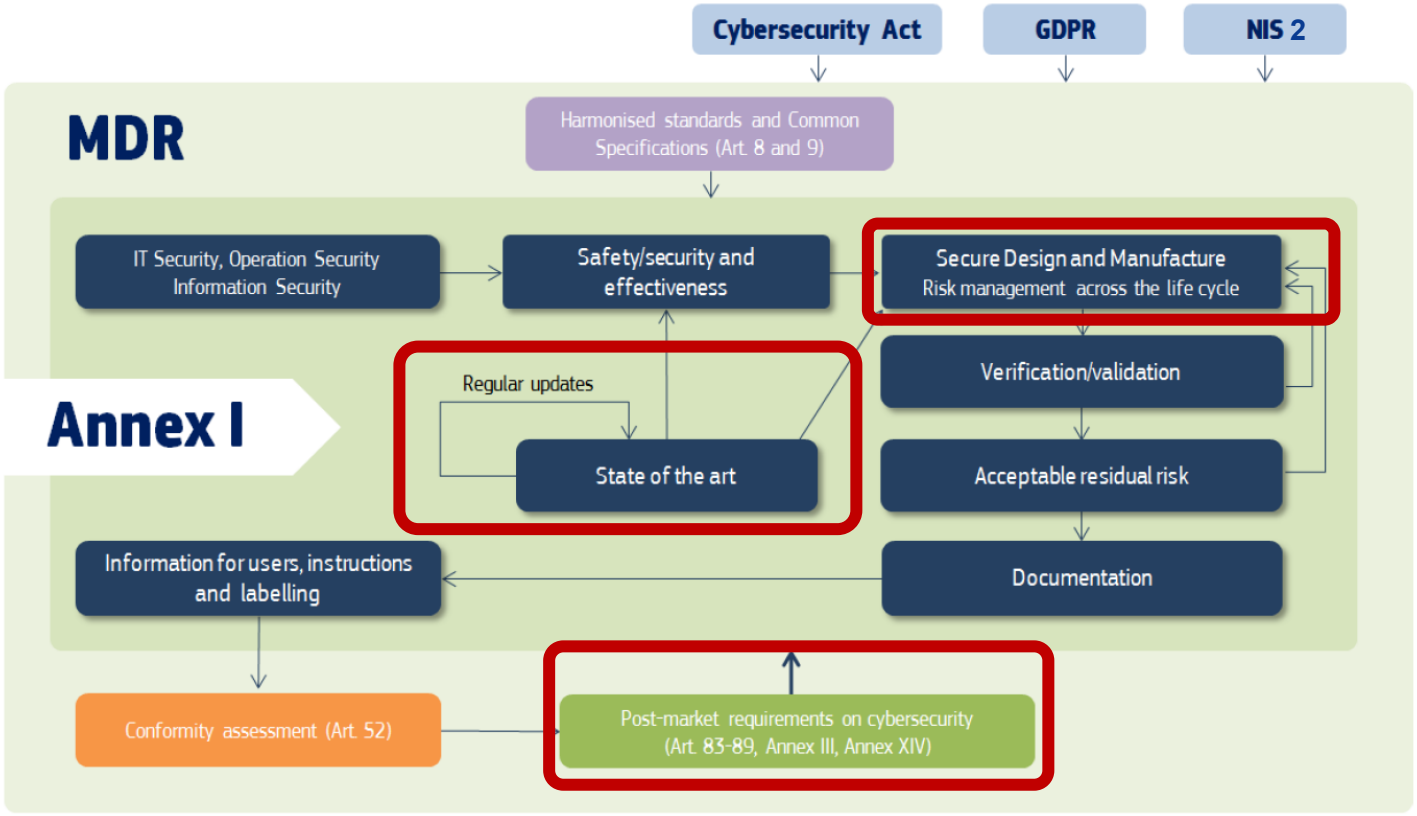
Market approval via authorized "Notified Bodies"; review documentation and will test

Cybersecurity included in audits; sampling for testing



Compliance with "Harmonized Standards" is enforced (e.g., IEC 81001-5-1)

Cybersecurity under EU MDR/IVDR



MDCG 2019-16 Guidance on Cybersecurity for medical deices; December 2019; July 2020 rev.1
https://ec.europa.eu/docsroom/documents/41863

Postmarket Cybersecurity Management under EU MDR/IVDR

Pre-market activities	Post-market activities
Secure Design (Annex I)	
Risk management (Annex I)	Risk management (Annex I)
Establish Risk Control Measures (Annex I)	Modify Risk Control Measures /Corrective Actions/Patches (Annex I)
Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex I)	Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex I)
Technical Documentation (Annex II and III)	Maintain and update a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)
Conformity Assessment (Article 52)	Trend Reporting (Article 88)
Establish a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)	Analysis of Serious Incidents (Article 89)
Clinical evaluation process (Chapter VI)	Post-Market Surveillance Report (Article 85)
	Periodic Safety Update Report (Article 86)
	Update Technical Documentation (Annex II and III)
	Inform the Electronic System On Vigilance (Article 92)

Global Trends Impacting Medical Device Cybersecurity

Over the past decade, regulators and lawmakers have raised the bar on cybersecurity:

General Corporate Responsibility and Reporting:

US Federal Agencies Reporting Requirements: SEC, FTC, CISA
US Government Federal Acquisition requirements
EU: NIS2, Cyber-Resilience-Act (CRA)

Personal Data Protection & Privacy:

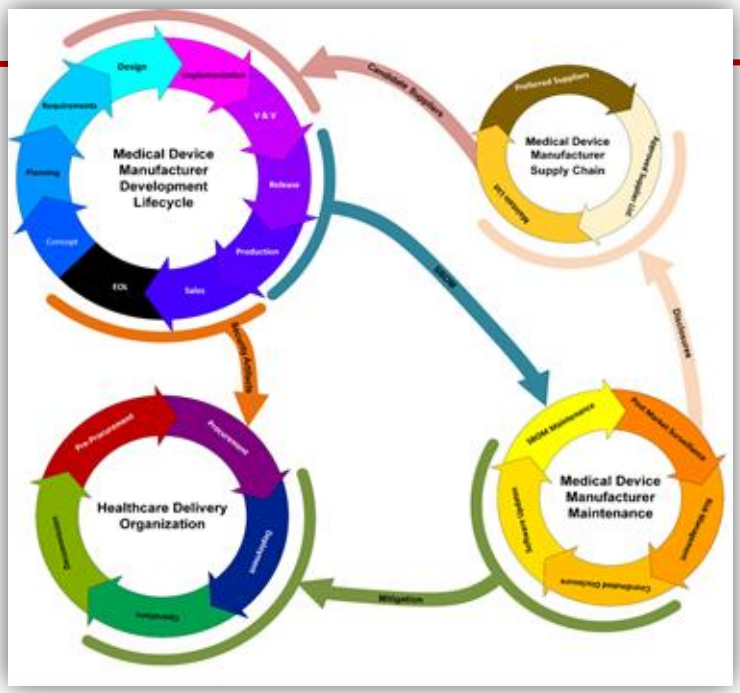
GDPR (EU), HIPAA (US) expecting update soon (?)
US State requirements for security and privacy: e.g., CA and CO now including “neural data”!

Medical Device Cyber-Safety:

US FDA Pre- and Postmarket Cybersecurity Guidances
MDR/IVDR – MDCG 2019-16
Australia TGA (appreciated for its technical detail) – Medical Device Cyber Security Guidance for Industry
Singapore (novel but solid approach to risk assessment) – TR 67:2018, Connected Medical Device Security
Health Canada - Pre-market Requirements for Medical Device Cybersecurity
IMDRF – Principles and Practices for Medical Device Cybersecurity
Many others: Japan, China, Saudi Arabia, …..

Wrapping up the Course

Hopefully, you won't fall for this anymore



Hopefully, this hangs on the wall by your desk

Thank you!

axel@medcrypt.com