WWW.24X7MAG.COM

24×7

THE VOICE OF HTM

SEPTEMBER/OCTOBER 2026

VOLUME 31 • NUMBER 5

SPECIAL CYBERSECURITY ISSUE



Expand Your Access

Where

HEALTHCARE CYBERSECURITY

Stands in 2026

Where the biggest risks—and HTM's role in addressing them—stand today

The Rise of the Cyber Biomed
Meet HTM's Emerging Cyber Specialist

Cybersecurity Enters the Buying Cycle
Why Security Is Moving Upstream

Cybersecurity Software Systems
2026 Comparison Guide

Inside a Medical Device Cyber Incident Response
What Happens When a Device Is Compromised

One probe restored

Countless lives touched





Elevate Patient Care

Rely on Innovatus Imaging

NSF

NSF-ISR

Registered to ISO 13485

844-687-5100

innovatusimaging.com

INNOVATUS imaging

SEPTEMBER/OCTOBER 2026 • VOLUME 31 • NUMBER 5

TABLE OF CONTENTS

24x7 THE VOICE OF HTM









Cover Photo:
ID 330739301 © AminaDesign | Dreamstime.com

FEATURES

6 WHERE HEALTHCARE CYBERSECURITY STANDS IN 2026
Hospitals and device manufacturers have more cybersecurity guidance and requirements than ever, but third-party attacks, AI-assisted vulnerability discovery, and aging equipment continue to complicate risk reduction.

12 CYBERSECURITY ENTERS THE BUYING CYCLE
Cybersecurity is entering medical device purchasing earlier as HTM teams scrutinize vendor support, contract terms, and long-term security risks.

22 THE RISE OF THE CYBER BIOMED
A new career path is taking shape as employers and training programs formalize the biomed cybersecurity specialist role.

DEPARTMENTS

4 EDITOR'S MESSAGE
Why a Special Issue on Cybersecurity?
By Alyx Arnett

10 CE PERSPECTIVES
Why Medical Device Cybersecurity Needs HTM Expertise
By Scott Trevino

16 FOCUS ON
Securing the Biomedical Network
By Dan Miles

18 CE PERSPECTIVES
HTM Workflow Tweaks to Secure Devices
By Phil Englert

20 SERVICE SOLUTIONS
You Can't Patch Everything
By Shankar Somasundaram

26 INDUSTRY INSIDER
The Next Cyberattack May Start With a Trusted Vendor
By William Hale

29 MANAGEMENT STRATEGIES
Continuous Compliance for Connected Medical Devices
By Kaarthick Subramanian

32 VIEWPOINT
The Reality of Rural Clinical-System Cybersecurity
By Don Seven

35 IN PRACTICE
Inside a Medical Device Cyber Incident Response
By Tamra Durfee

48 COMPARISON GUIDE
Cybersecurity Software Systems

CYBERSECURITY REPORT

38 Cyber Resilience Program Puts Clinical Continuity in HTM's Sights

40 HSS Cyber Module Draws Steady Uptake from Health Systems

42 Inside Siemens Healthineers' $6.9M Medical Device Cybersecurity Research Project

46 CHAI's Push to Build Healthcare's First Playbooks for Frontier AI Cyber Risk

SUBSCRIBE Stay up to date on the latest in HTM with news delivered straight to your inbox. Sign up for our newsletters at https://info.medqor.com/24x7subform

24x7
THE VOICE OF HTM

PRESIDENT/PUBLISHER
JOE DEL GROSSO
(347) 456-6019
jdelgrosso@medqor.com

CHIEF EDITOR
ALYX ARNETT
(913) 278-0194
editor@24x7mag.com

ART DIRECTOR | STALIN ANNADURAI

MEDQOR™
7300 W 110th St, Fl 7,
Overland Park, KS 66210
(913) 955-2600
MEDQOR.COM

OWNER/FOUNDER | BRIAN WEAVER

CHIEF EXECUTIVE OFFICER | DON RANSDELL

CHIEF TECHNOLOGY OFFICER | RICHARD SOARES

VP, OPERATIONS | TONYA MANNING

VP, DATA OPERATIONS | PAM AYERS

24x7 is the resource HTM professionals have relied on for more than 20 years to deliver complete coverage of tech, regulatory, and industry trends, as well as managerial advice.

***24x7** Magazine* (ISSN 1091-1626) is published bi-monthly by MEDQOR LLC, 7300 W 11th St. Fl 6, Overland Park, KS 66210. September/October 2026, Vol 31 No. 5. All rights reserved. No part of this publication may be reproduced in any form without written permission from the publisher. Entire contents ©2026 by MEDQOR LLC. POSTMASTER: While the publishers have made every effort to ensure the accuracy of the materials presented in 24x7, they are not responsible for the correctness of the information and/or opinions expressed.

E-Mail: 24x7custsrvc@medqor.com
Phone: (913) 278-0161
Fax: (913) 894-6932
Mail: 7300 W 110th St, Fl 7, Overland Park, KS 66210

LIST RENTAL:
Statlistics: (203) 778-8700; www.statlistics.com

AMERICAN BUSINESS MEDIA
The Association of Business Media Companies

WHY A SPECIAL ISSUE ON CYBERSECURITY?



Alyx Arnett

Medical device cybersecurity has given us plenty to cover this year. Cyber incidents have hit hospitals and health systems directly, while attacks on medical device manufacturers and other vendors have shown how disruption can also come through third parties. FDA cybersecurity requirements are continuing to shape how manufacturers develop and support connected devices, and hospitals are facing newer questions around AI and how to plan for prolonged cyber disruptions to clinical care.

That's why we decided to devote this special issue of *24x7* to cybersecurity. The stories in these pages look at the issue from several angles, but they have one thing in common: HTM has a role in all of them.

A few numbers from recent reports show what hospitals are dealing with:

- **24%** of organizations surveyed for RunSafe Security's 2026 Medical Device Cybersecurity Index reported a cyberattack or exploited vulnerability involving a medical device, up from 22% in 2025.
- Among those organizations, **80%** said the incident had a moderate or significant impact on patient care.
- **56%** said their organization has rejected a medical device because of cybersecurity concerns.
- **28%** said their organization operates medical devices beyond the manufacturer's end-of-support date.
- And in Verizon's 2026 Data Breach Investigations Report, **32%** of healthcare breaches involved a third party.

Behind those numbers are some of the questions we wanted to dig into with this issue.

What actually happens when a medical device is involved in a cyber incident? How much weight should cybersecurity carry when a hospital is deciding which equipment to buy? How do HTM teams manage cyber risk that comes through vendors and other third parties? And what happens when a rural hospital is expected to meet the same cybersecurity demands as a major health system?

We also take readers inside a $6.9 million Siemens Healthineers research project aimed at strengthening medical device cybersecurity and explore the rise of the "cyber biomed," as HTM professionals take on roles that combine biomedical equipment expertise with cybersecurity. We look at continuous compliance for connected devices, securing the biomedical network, and new efforts to prepare hospitals to keep providing care when a cyberattack takes technology down.

We've also included a cybersecurity software comparison guide looking at tools available to healthcare organizations for managing these risks.

Not every hospital has the same resources, and not every HTM department will have the same role in cybersecurity. But the clinical and technical knowledge HTM professionals have is becoming increasingly important as healthcare works to secure a growing—and aging—inventory of connected technology.

We hope this issue gives you useful information for that conversation. ●

24X7 ADVISORY BOARD

Matthew F. Baretich, PE, PhD, President, Baretich Engineering, Fort Collins, Colo.

Roger A. Bowles, MS, EdD, CBET, Professor, Department Chair, Biomedical Equipment Technology, Texas State Technical College, Waco, Texas

Phil Englert, Vice President of Medical Device Security, Health-ISAC, Orlando, Fla.

Stephen Grimes, FACCE, FHIMSS, FAIMBE, Managing Partner, Strategic Healthcare Technology Associates

Wayne Hibbs, CCE, Principal, BSA LifeStructures, Indianapolis, Ind.

Gordon Hosoda, Chief, Healthcare Technology Management, VA Portland Health Care System, Portland, Ore.

Clarice M. L. Holden, BSE, Supervisory Biomedical Engineer, Dallas VA Medical Center, Dallas, Texas

Samantha Jacques, PhD, FACHE, Vice President, Clinical Engineering, McLaren Health Care

Paul Kelley, CBET, AAMIF, Director of Biomedical Engineering the Green Initiative and Asset Redeployment, Washington Hospital Healthcare System, Fremont, Calif.

Dennis Minsent, MSBE, CCE, CBET, Life Safety Code Surveyor, The Joint Commission

Ken Olbrish, MSBE, Senior Product Manager, Arthrex California Technology, Santa Barbara, Calif.

Jeffrey Ruiz, Technology Manager, Healthcare Technologies, TRIMEDX, Holland Hospital, Holland, Mich.

Elliot B. Sloane, PhD, CCE, Assistant Professor, Villanova School of Business, Villanova, Pa.

Arif Subhan, MS, CCE, Chief Biomedical Engineer, VA Greater Los Angeles Healthcare System

Dustin Telford, CHTM, CBET, CRES, CLES, Regional Biomedical Equipment Technician, Bio-Electronics, Principal, Healthcare Technology Strategies

Binseng Wang, ScD, CCE, FAIMBE, FACCE Consultant, BSI - Health Technology Consulting

Stay Ahead in Healthcare Technology

24x7

Get expert analysis, industry insights, healthcare technology news, and the latest innovations delivered right into your inbox.



Sign up for our free digital magazine & newsletters at 24x7mag.com/subscribe

WHERE HEALTHCARE CYBERSECURITY STANDS IN 2026

Hospitals and medical device manufacturers have more cybersecurity guidance and requirements than ever, but third-party attacks, AI-assisted vulnerability discovery, and aging equipment continue to complicate efforts to reduce risk.

By Alyx Arnett



In 2026, more healthcare organizations are reporting cyber incidents involving medical devices—and more of those incidents are affecting patient care, according to RunSafe Security's 2026 Medical Device Cybersecurity Index. The report found that 24% of organizations reported an attack or exploited vulnerability involving a medical device, up from 22% in 2025. Among organizations that experienced an incident, 80% said it had a moderate or significant effect on patient care, up from 75%.[1]

The risk is also reaching hospitals through companies they depend on, with third parties involved in 32% of confirmed healthcare breaches.[2] Scott Gee, deputy national advisor for cybersecurity and risk at the American Hospital Association, sees another source of pressure: Artificial intelligence (AI) is shortening the time attackers need to turn a disclosed software vulnerability into an exploit.

"Everything has gotten bigger and badder and more in your face," says Naomi Schwartz, vice president of services and regulatory strategy at MedCrypt and a former US Food and Drug Administration (FDA) reviewer.

For medical device manufacturers, those growing risks are accompanied by more specific cybersecurity guidance, while hospitals have gained new resources to assess their risks and prepare for disruptions to care. For Schwartz, the challenge is turning a growing volume of cybersecurity information into decisions hospitals can act on. "It's very hard" to keep up, she says.

CYBERSECURITY GUIDANCE EXPANDS ON BOTH SIDES OF THE DEVICE

While risks are increasing, the good news is that the FDA's recently updated final cybersecurity guidance and Section 524B of the FD&C Act have "significantly raised expectations" for medical device manufacturers, says Priyanka Sollinger, CHTM, DSL, AAMIF, FACCE, vice president of cybersecurity and risk reduction services at Asimily.

"They now have responsibilities around securely deploying these devices, postmarket vulnerability management, and then having a good patching strategy," she says. Section 524B also requires manufacturers submitting covered cyber devices for premarket review to provide a software bill of materials (SBOM).

Expectations for that information are spreading globally. The International Medical Device Regulators Forum published principles for medical device SBOMs in 2023. In July, CISA and government partners from eight other countries updated the minimum elements for SBOMs.



Photo credit: ID 71953800 © Sudok1 | Dreamstime.com

Top Cybersecurity Risks

Health sector CISOs identified these as their leading cybersecurity risks in Health-ISAC's 2026 benchmarking report:

81% Phishing / Social Engineering

64% Supply Chain / Third-Party Risk

60% Ransomware / Malware

*Health-ISAC's 2026 CISO Benchmarking Report

"It's not the United States government and CISA focusing on software bill of materials," Schwartz says. "It's the whole world, effectively."

RunSafe's report found that 81% of respondents considered an SBOM important or essential when evaluating devices; 35% said they would not consider a device without one.[1]

Hospitals have also received new resources for assessing and responding to cyber risks. In March, the US Department of Health and Human Services (HHS) added a cybersecurity module to its RISC 2.0 toolkit, allowing healthcare organizations to assess cyber threats alongside other hazards. HHS also updated its Security Risk Assessment Tool, which is intended primarily for small and medium providers.

Gee points hospitals to the FBI's Operation Winter SHIELD, released this year. Its 10 recommended defenses draw on weaknesses seen in FBI investigations. The American Hospital Association and Joint Commission also launched a voluntary Cyber Resilience Readiness program in May to help hospitals assess their ability to sustain safe, quality care during cyber disruptions.

THE HIPAA PROPOSAL RAISES QUESTIONS

The proposed HIPAA Security Rule update, intended to strengthen cybersecurity protections for electronic protected health information, could go further by setting more specific requirements for hospitals.

"The HIPAA law needs to be updated," Schwartz says. "Absolutely, it is stale. There are a bunch of things it doesn't cover."

Still, stakeholders have raised concerns about how some provisions work. For one, it would remove the distinction between "required" and "addressable" implementation specifications, making most specifications mandatory with limited exceptions, says Eddie Myers, HCISPP, CBET, national director of cybersecurity at Intelas. "A lot of hospitals are saying, 'OK, yes, we don't have the bandwidth to do that,' but they're making it mandatory," Myers says.

It would also require network segmentation. "Many organizations understand segmentation conceptually—that they should segment medical devices," says Sollinger. "But now translating thousands of those device communication patterns into enforceable network policies, and then doing all of that without disrupting patient care or annoying your clinicians, that's going to be difficult."

Recovery raises a separate concern. The proposed rule calls for written procedures to restore critical relevant electronic information systems and data within 72 hours of their loss. "I don't know anybody that can do that, government agencies included," says Gee. "Within the first 72 hours, you're quite often still trying to figure out what happened, how it happened, how the bad guys got in, and make sure they're not in anymore."

Gee says he supports stronger cybersecurity measures but that the proposed requirements must be workable for hospitals. HHS issued the proposal in December 2024; the federal regulatory agenda now projects final action in July 2027. Meanwhile, Sollinger cautions against treating the delayed rulemaking as a reason to wait.

"Just because it is still proposed doesn't mean it's not coming," she says.

THIRD-PARTY RISKS ARE AT THE FRONT DOOR

According to Gee, "The biggest challenge we see in the sector writ large right now is and continues to be third-party risk."

Verizon's 2026 Data Breach Investigations Report found third-party involvement in 32% of confirmed healthcare breaches.[2] A separate 2026 study found that 85% of healthcare practices experienced at least one operational disruption caused by a third-party or "vendor-of-a-vendor" failure during the past 12 months.[3]

Gee points to recent examples like the March cyberattack on Stryker that disrupted the manufacturer's order processing, manufacturing, and shipping. In August, a cyber incident at Boston Scientific affected manufacturing and order fulfillment, along with the activation of some cardiac remote-monitoring devices.

80%

Of organizations that reported a medical-device cyber incident or exploited vulnerability, 80% said it had a moderate or significant effect on patient care.

Neither incident began inside a hospital's network, but hospitals still had to consider their dependence on the manufacturers. Myers says the Stryker incident prompted Intelas to identify potentially affected devices across its clients' inventories and evaluate their remote connections. Where disabling remote access would not interfere with patient care, the company recommended turning off those connections until the manufacturer provided an all-clear.

Third-party risk also extends to the companies that provide hospitals with billing, software, and IT services. Gee points to the 2024 attack on claims and payment processor Change Healthcare and an incident at healthcare software provider Craneware as examples.

Health-ISAC's 2026 threat report identifies medical billing, software, IT support, and file-transfer providers among the outside companies attackers target.[4]

AI CHANGES THE THREAT AND THE RESPONSE

AI is adding to the risk by helping attackers exploit newly disclosed vulnerabilities faster, Gee says. Before AI, he says, an attacker might have needed weeks to develop an exploit. "With AI, they're doing it in minutes. AI is incredibly good at determining what vulnerabilities are and how to exploit them," he says.

AI could also add to the number of flaws demanding attention. In April, Anthropic reported that its Claude Mythos Preview model had found thousands of previously unknown software vulnerabilities. Anthropic has made the model available to selected defenders through Project Glasswing. For Myers, the finding is a reminder that even recently installed devices may have security weaknesses no one has discovered yet.

And, finding a vulnerability is only the beginning of the

response, Schwartz says. A manufacturer must evaluate a fix and test it before releasing a patch. "And that's not fast," she says.

To help hospitals respond to attackers using increasingly capable AI, the Coalition for Health AI convened a nearly 100-member work group earlier this year. It is developing cybersecurity playbooks for health systems, with guidance expected by the end of 2026.

While AI may be speeding attacks, it can also help defenders. Sollinger says security and healthcare technology management (HTM) teams are using it to analyze device, network, and vulnerability data and identify risks that need attention. "We have enormous amounts of data … It's just impossible for a human to do it all," she says.

Additionally, AI brings risks through the medical devices and clinical systems hospitals are using, Sollinger says. RunSafe's report found that 57% of respondents' organizations used AI-enabled or AI-assisted medical devices or clinical systems, and 80% expressed at least moderate concern about the associated cybersecurity risks.[1]

"It's here; we're not stopping it, but we need to have a governance structure in place for how to use it appropriately," Gee says.

THE SECURITY CHALLENGE OF LEGACY DEVICES

Hospitals have become better at identifying connected devices and their vulnerabilities, Sollinger says. "But then knowing that something is vulnerable and then being able to remediate that vulnerability are two very different things."

That difficulty is particularly stark with older equipment. "In our world, HTM, we're there to extend the useful life of the device," Myers says. That often leaves teams maintaining equipment with outdated software or devices that have reached the end of manufacturer support.

RunSafe's report found that 28% of respondents said their organizations operate medical devices beyond the manufacturer's end-of-support date.[1] Among organizations with legacy equipment, 39% reported using it in emergency departments, 36% in intensive care units, and 33% in operating rooms and procedure suites.[1]

Asked why they continued using vulnerable devices, 38% said no acceptable replacement was available, 36% cited cost, 34% cited regulatory or approval constraints, and 33% said replacement would cause too much disruption.[1] Nearly one-quarter said the manufacturer had not provided an upgrade path.[1]

Schwartz says large imaging systems are often among the older devices hospitals may need to keep in service as replacing an MRI, for example, can take years of budgeting, and installing a new one can require substantial construction. "They need to figure out, is there a way to bubble wrap that thing from a cybersecurity perspective to keep it operating as long as they can," Schwartz says. "We have to find defensive measures for older stuff, and we have to really focus on secure by design for anything new."

One such measure is runtime exploit protection, which is designed to block attacks on vulnerable software without requiring a patch. Among 419 respondents familiar with the technology in RunSafe's survey, 82% said their organizations had deployed or were piloting it: 29% widely and 53% on some devices.[1]

Schwartz says older devices also pose a question for manufacturers: Should they still be selling them? In Japan, medical device manufacturers have had to demonstrate conformity with cybersecurity principles based on JIS T 81001-5-1 since April 2024. She says the framework calls for reassessing "transitional health software"—products developed before current secure-development practices—and identifying additional controls where needed.

"In Japan, they may actually literally tell you, 'Get that old thing off the market right now. Take it out of the hospitals,'" Schwartz says.

Schwartz expects other countries to take a closer look at older products, too. "I don't think that that is going to be an outlier for very long," she says.

"THE BIGGEST CHALLENGE WE SEE IN THE SECTOR WRIT LARGE RIGHT NOW IS AND CONTINUES TO BE THIRD-PARTY RISK."
— Scott Gee, American Hospital Association

CYBERSECURITY PLANNING SHIFTS TOWARD CLINICAL CONTINUITY

Hospitals cannot patch every vulnerability or prevent every disruption, Sollinger says. That is putting more emphasis on limiting an incident's effects and protecting the systems most critical to patient care.

"Hospitals need to understand that devices are going to have vulnerabilities," she says. "There are going to be new vulnerabilities discovered, and you can't probably patch all of them. You can't control the risk with all of them."

Gee says teams need plans to keep providing safe care if a cyberattack or other outage takes essential technology offline. Joint Commission and American Hospital Association's new Cyber Resilience Readiness program gives hospitals a way to assess their ability to maintain care in such an event. "The time to figure out how to do that is not during an incident," he says. "What we encourage is build those plans and practice."

Sollinger says HTM professionals have a role in those decisions because they know what the equipment does and how clinicians rely on it. For her, that reflects a change in how the field understands medical device cybersecurity.

"Ultimately, we're moving from medical device security just being viewed as a specialized security problem to now being recognized as a core component of patient safety," she says. ●

- Alyx Arnett is chief editor of 24x7 *Magazine.*

REFERENCES

1. RunSafe Security. RunSafe Security's 2026 medical device cybersecurity index: Insights from healthcare decision-makers on medical device procurement, risk, and resilience. Published 2026. Accessed 2026 Sept 17.
2. Verizon. 2026 Data breach investigations report: Healthcare snapshot. Published 2026. Accessed 2026 17 Sept.
3. Omega Systems. Under pressure: The 2026 healthcare IT landscape report. Published 2026. Accessed 2026 Sept 17.
4. Health-ISAC. 2026 Global health sector threat landscape. Published 2026. Accessed 2026 Sept 17.



WHY MEDICAL DEVICE CYBERSECURITY NEEDS HTM EXPERTISE

HTM professionals bring critical clinical context to medical device cybersecurity, but the growing role also requires new skills and training.

By Scott Trevino, senior vice president of cybersecurity, Trimedx

Healthcare technology management (HTM) has always focused on keeping medical equipment safe, reliable, and available for patient care. That mission remains the same, but the way HTM teams achieve it is evolving.

Medical device cybersecurity is no longer solely the responsibility of IT teams. As new vulnerabilities emerge, health systems need to understand which devices are affected, how critical those devices are to patient care, and which risks require immediate attention. Doing so depends on pairing cybersecurity expertise and technology with clinical engineering knowledge and experience—neither is sufficient alone.

BRINGING CYBERSECURITY AND CLINICAL EXPERTISE TOGETHER

Biomedical equipment technicians (BMETs) understand each device's clinical context, helping ensure remediation efforts do not disrupt patient care. Pairing that knowledge with vulnerability intelligence and risk-based prioritization helps organizations focus on the issues that matter most. From there, teams can act—applying validated patches, using compensating controls where no patch exists, and measuring risk reduction as part of a true

By The Numbers

Medical device inventories can be inaccurate by as much as 40% before reconciliation, according to TRIMEDX internal data—a gap the company says can undermine medical device cybersecurity efforts.

*Trimedx's 3 Essential Steps to Improve Medical Device Cybersecurity white paper

closed-loop remediation process.

The most prepared health systems will prioritize equipping BMETs with the cybersecurity skills they need to successfully work in today's threat environment. Training programs and professional development opportunities should incorporate cybersecurity fundamentals, risk management concepts, and cross-functional collaboration skills alongside traditional technical competencies.

The line between clinical engineering and cybersecurity is thinning, and the people entering the field will not experience them as separate disciplines the way their predecessors did. Cybersecurity is a necessary skill for HTM. Organizations that invest in that education now will have HTM teams capable of the work the role demands, rather than scrambling to hire it later.

USING AI TO SUPPORT HTM EXPERTISE

As HTM professionals take on a greater role in cybersecurity, they also face an increasing volume of data to interpret and act on as connected device inventories grow and new vulnerabilities are identified every day. AI has the potential to help teams make sense of that information faster by providing easier access to cybersecurity insights, automating routine analysis, and helping prioritize actions based on risk.

One example is the use of conversational AI tools that allow users to ask natural-language questions about medical device inventory, vulnerabilities, risk scores, remediation efforts, and overall cybersecurity posture. These capabilities can surface high-risk assets and generate reports on demand, without navigating multiple systems or manually analyzing data.

AI can also correlate newly discovered vulnerabilities with device inventories, making it easier to identify affected assets, support more dynamic risk assessments, and take a more proactive approach across the device lifecycle.

Used well, AI should raise the value of human expertise by putting sharper information in the hands of the people who understand each device and the impact it has on patient care.



Scott Trevino is senior vice president of cybersecurity at Trimedx. He leads efforts to define the strategy to deliver value, growth, and evolution of Trimedx's cybersecurity solutions.

LOOKING AHEAD

Medical devices will keep getting smarter, and the threats against them will keep pace. The health systems that handle it best will be the ones that stop treating cybersecurity solely as a separate specialty and build it into how their HTM teams are trained, staffed, and equipped.

For HTM, cybersecurity is no longer adjacent to the work of keeping equipment safe, reliable, and available. It is an essential part of it. ●





Photo credit: ID 465062173 © Vadzim Shubich | Dreamstime.com

CYBERSECURITY ENTERS THE BUYING CYCLE

Cybersecurity considerations are coming earlier in medical device purchasing as HTM teams look more closely at vendor support, contract terms, and long-term security risks.

By Alyx Arnett

Cybersecurity is becoming an increasingly important part of medical device purchasing, and healthcare technology management (HTM) teams are more often considering potential risks earlier in the buying process, according to Scott Skinner, PhD, MBA, FACHE, CHTM, founder and principal of consulting firm HTMPOWER.

"For years, as we've evaluated technologies, we've certainly looked at the clinical features, reliability, supportability, and total cost of ownership. But we've got to the point now where the cybersecurity elements are really one of the main criteria," says Skinner, also an assistant professor of health management and systems sciences at the University of Louisville.

Those considerations are increasingly influencing purchasing decisions. RunSafe Security's 2026 Medical Device Cybersecurity Index found that 84% of organizations include cybersecurity requirements in vendor requests for proposals, while 56% have rejected a device because of cybersecurity concerns, up from 46% in 2025.

For Skinner, the timing of that evaluation is key. "I think originally everybody was sort of treating this as a checklist that you do right before you give the vendor the purchase order (PO)," he says. "Well, if that's where it is in the process, it's way too late. Cybersecurity needs to have a seat at the table right from the very beginning."

WHY CYBERSECURITY IS MOVING EARLIER

Katie Conner, senior director of cybersecurity at Intermountain Health, says the inclusion of cybersecurity in procurement decisions reflects how much the device landscape has changed.

"Medical devices used to be really just on their own and operate in a silo, and they would plug into the wall and not be interconnected. The interconnectivity of medical devices today is more critical than ever and more prevalent than ever," Conner says. "It's no longer an option for a medical device to just show up, and you plug it in and start operating it."

Scott Trevino, senior vice president of cybersecurity at Trimedx, points to another factor accelerating the shift: the pace of attacks.

"The growing volume and speed of cyberattacks, particularly AI-enabled attacks, have heightened the urgency of evaluating cybersecurity during the medical device purchasing process," he says.

Regulatory expectations are adding to the pressure. The RunSafe

survey found that 79% of respondents said US Food and Drug Administration guidance or EU Medical Device Regulation requirements have influenced their medical device procurement practices.

WHERE HTM FITS IN

Skinner says HTM's position between clinical staff, IT, and manufacturers gives the department an important role in evaluating devices for cybersecurity.

"We're really good at relating with the clinicians and the users because we're responsible for supporting the physical device. We often have to collaborate with technical teams to bring things onto the network to do commissioning, work through patching and cyber events, and we're really good at relating with the manufacturer for service and support," he says.

That position often makes HTM a translator between groups that don't necessarily speak the same technical language, Skinner says.

"The clinicians don't always understand the language that IT, for example, is speaking in. And we may not be IT experts, but we often have an operating knowledge that makes us able to functionally relate to IT to get things done for medical devices," he says.

Conner also describes HTM as a bridge between vendors and the teams that will support the technology.

"When they can come in and help us understand how the device will actually be implemented, deployed, maintained, and supported in the patient care environment … we can then ensure security is embedded in that design and that plan," she says.

WHAT TO ASK FOR—AND WHAT TO WATCH FOR

Trevino says HTM teams should start by obtaining key cybersecurity information from the manufacturer. "HTM teams should request MDS2 forms, SBOMs, and documentation outlining any known vulnerabilities affecting a device," he says. "They should also review vulnerability disclosures and confirm whether identified vulnerabilities have been patched or mitigated before deploying the device."

The RunSafe Index found that 81% of respondents rate an SBOM as "important" or "essential," and 35% say they will not consider a device without one.

Additionally, Skinner says, "Teams should ask whether they have a documented process to respond to security events that addresses notification timelines and transparency, as well as the regulations, standards, and guidance that inform their response approach."

He says HTM teams should also be asking vendors how the device's operating system will be supported over its expected life. That includes whether the operating system already has an established end-of-life or end-of-service date and whether the manufacturer will provide a path to a newer operating system.

"What's the plan look like for when we get to that seven to 10 years? Is there going to be an upgrade path to move to the next operating system?" he says.

Conner says teams should also ask how the manufacturer handles vulnerabilities after a device is in use, including how quickly vulnerabilities are disclosed and addressed and how the vendor approaches patches and updates.

"We expect vulnerabilities to happen, but how are they going to respond and support us in achieving better vulnerability management? What's their patching update processes, and really, how do they support the lifecycle of the device end to end?" she says.

The vendor's response to those questions can itself be revealing, Conner says. "The biggest red flags are when a vendor is not willing to cooperate, doesn't really understand the question set around security," she says. "You get a pretty good idea pretty early on as to the security posture of a vendor and their willingness to participate in security."

GETTING REQUIREMENTS INTO THE CONTRACT

Once an organization has identified its cybersecurity requirements, Skinner says those expectations need to be addressed before the contract is finalized and the purchase order (PO) is issued.

"If you have leverage until you consummate the contract and until you cut the PO, that's where there just needs to be a lot of partnership internally," he says. "We need to make sure that we get those requirements baked into the contract terms and conditions and in the actual PO before we let the horse out of the barn because then it's too late, and we don't have any leverage with the manufacturers."

Teams may want to have patching timelines included, for example. "If we want to see, like within one week in general, the patch is tested and validated and allowed to be pushed and we somehow want the manufacturer to work with us on that, then those are elements that should be baked into the contract," Skinner says.

Conner says contracts should also spell out who is responsible for maintaining the device's security after purchase.

"Oftentimes there's confusion about who will be actually patching the systems," she says. "Will it be us, and we're waiting for a patch from the vendor, and the HTM team will help to apply that once it is available? Or will the vendor need to log in remotely and support updating, patching critical vulnerabilities? And are there additional costs required to do that?"

Trevino says a vendor's track record can also influence what an organization requires in the contract.

"Past experiences with a vendor's support and responsiveness

By the Numbers

76% of healthcare decision-makers surveyed by RunSafe Security said they would pay a premium for medical devices with advanced cybersecurity protections, with 49% willing to pay at least 5% more.

*RunSafe Security's 2026 Medical Device Cybersecurity Index

can influence purchasing decisions and drive organizations to seek stronger cybersecurity commitments within purchase contracts," he says.

DOES CYBER RISK MEAN IT'S TIME TO REPLACE?

For hospitals operating older or unsupported medical devices, cybersecurity can raise another purchasing question: Is it time to replace them? The RunSafe Index found that 28% of organizations operate devices past end-of-support, while 44% acknowledge running end-of-support devices with known, unpatched vulnerabilities.

But replacing those devices with newer equipment isn't necessarily an automatic cybersecurity improvement, Skinner says.

"Sometimes replacing something isn't going to change that risk profile a whole lot," he says. "I think sometimes we assume that, 'Oh, this thing's a really high risk. It's running on Windows XP. We just need to get a new one and bring it in.' Well, hold on … the new device may be as bad or worse from a compliance standpoint with the environment."

At the same time, Conner says some medical equipment can remain clinically useful long after its software becomes difficult to support securely. She points to large imaging systems as an example.

"We have some very large imaging systems out there, and many of them last for 20 years or 30 years, or longer," she says. "The hardware itself would work, and the device itself would work much longer than the integration into the system securely."

For Skinner, that makes cybersecurity one consideration in replacement planning, not a reason to assume that purchasing a newer device will solve the problem. The proposed replacement still needs to be assessed for its own risks, he says.

"There may be things that are fundamental around how the device is designed that may not have changed," he says. "So I think just coming in and saying, 'Oh, we need to replace all this, and it's going to drive our risk down.' Well, you really need to do the assessment and really see if that's true or not."

For organizations that cannot immediately replace an unsupported device, compensating controls may provide another option. The RunSafe Index found that 82% of organizations have deployed or are piloting runtime exploit protection, including 53% that have deployed it on some devices and 29% that have deployed it widely. The report identifies such protections as an option for devices that cannot be patched or replaced.

PUSHING VENDORS—TOGETHER

Healthcare organizations are increasingly using their purchasing decisions to hold manufacturers accountable for cybersecurity, says Trevino.

"In some cases, healthcare organizations have reconsidered purchasing from a vendor after experiencing issues such as being charged for security patches or receiving insufficient support for maintaining device cybersecurity," he says. "Even when organizations continue purchasing from the same manufacturer, those past experiences often lead to stronger contract language requiring patch support and cybersecurity maintenance commitments."

The RunSafe Index shows that those experiences are affecting vendor relationships more broadly. Nearly 40% of organizations said cybersecurity incidents have affected their trust in specific vendors and led them to require additional verification, up from 32% in 2025. Seven percent said they have stopped purchasing from specific vendors entirely, while 23% said they are exercising greater caution when evaluating vendors.

> **"CYBERSECURITY NEEDS TO HAVE A SEAT AT THE TABLE RIGHT FROM THE VERY BEGINNING."**
> — Scott Skinner, PhD, MBA, FACHE, CHTM, founder and principal, HTMPOWER

Hospitals are also willing to put more money behind stronger security. The index found that 76% of respondents would pay a premium for devices with advanced cybersecurity protections, including 49% who would pay at least 5% more.

Conner says that purchasing pressure becomes more powerful when healthcare organizations apply it collectively.

"[In some security conversations with manufacturers], they'll say, 'This is the first time I'm hearing this. Nobody else is making us fix this.' And that's just simply not true," she says. "All of us in healthcare are pushing on the vendors to improve to ensure that they are doing their part as part of our healthcare systems to support us."

Conner says she has also seen larger healthcare organizations work directly with manufacturers to identify security problems, including conducting penetration testing on medical devices and connected software and sharing what they find with vendors. She says that type of collaboration can help manufacturers address problems that extend beyond a single healthcare system.

WHAT COMES NEXT

Looking ahead, Conner expects healthcare organizations to require more from manufacturers. "We're moving really from asking manufacturers and vendors if the device is secure to really having them demonstrate how security will be maintained throughout the device's lifecycle and making sure that we address that in contract terms," she says.

AI-enabled devices will add more considerations to that evaluation. The RunSafe Index found that 57% of organizations already use AI-enabled or AI-assisted medical devices, and 80% express at least moderate concern about the cybersecurity risks they introduce. Conner says procurement teams will need to consider data integrity, model risk, privacy, and resilience as AI becomes more embedded in medical technology.

Ultimately, she says the purchasing process is about understanding those risks upfront and making sure they can be managed over time.

"We do expect there to be risks. There's always going to be risks, and the threat landscape is evolving our risk posture over time," Conner says. "So the goal is not to be 100% secure. The goal is to be able to manage those risks over time as partners and make sure that we're securing and protecting our healthcare ecosystem overall." ●

- Alyx Arnett is chief editor of 24×7 *Magazine.*

24x7

A MEDQOR BRAND

WANT MORE?

Check out our digital edition at
24x7mag.com/magazine-archive
for this issue and all archived editions





Photo credit: ID 22308837 © Mikhail Popov | Dreamstime.com

SECURING THE BIOMEDICAL NETWORK: BUILDING A FOUNDATION FOR SAFE, CONNECTED HEALTHCARE

A layered cybersecurity strategy can help healthcare organizations protect connected medical devices without disrupting clinical operations.

By Dan Miles, vice president of information technology at Intelas

Today's hospitals depend on thousands of connected medical devices to deliver patient care. Infusion pumps, patient monitors, imaging systems, anesthesia machines, and laboratory equipment all communicate across the healthcare network. While this connectivity improves clinical workflows, it also expands the organization's cybersecurity risk.

The challenge is no longer simply protecting computers. Healthcare organizations must now secure an ecosystem of interconnected clinical devices while ensuring uninterrupted patient care.

The goal should be to reduce cyber risk without negatively impacting clinical operations.

NETWORK SEGMENTATION: THE FIRST LINE OF DEFENSE

One of the most effective ways to reduce risk is through network segmentation.

Rather than allowing medical devices to reside on the same network as administrative systems, hospitals should isolate biomedical devices into dedicated network segments based on clinical function and risk.

Effective segmentation not only helps to limit lateral movement during a cyberattack, but it also



Dan Miles is vice president of IT at Intelas, where he leads strategic and operational technology initiatives across the organization.



reduces the stack surface and improves visibility into device communications.

Network segmentation should be considered a foundational cybersecurity control rather than an optional enhancement.

CONTROLLING REMOTE VENDOR ACCESS

Many medical devices require remote vendor support for software updates, diagnostics, and maintenance.

Unfortunately, unmanaged remote access has become one of the largest attack vectors within healthcare. Every remote connection should be treated as privileged access.

Here's a checklist for what organizations should require to ensure cyber safety:

- Multi-factor authentication (MFA)
- Time-limited access windows
- Approval workflows
- Session logging
- Least-privilege access
- Vendor accountability

MULTI-FACTOR AUTHENTICATION IS NO LONGER OPTIONAL

Passwords alone cannot adequately protect healthcare environments. MFA should be implemented for biomedical technicians, clinical engineering leadership, third-party vendors, service providers, and administrative users.

Modern identity platforms make it possible to enforce MFA without creating unnecessary operational burdens.

VISIBILITY IS THE MISSING PIECE

Hospitals often own thousands of medical devices, yet many organizations cannot answer simple questions:

- Which devices are connected today?
- Which devices contain critical vulnerabilities?
- Which devices have reached end of support?
- Which systems are affected by the latest FDA recall?

Without centralized visibility, organizations are forced into reactive security.

Modern healthcare technology management (HTM) platforms should integrate cybersecurity data, asset inventories, vulnerability management platforms, and FDA recall information into a single operational view.

FROM CYBERSECURITY TO OPERATIONAL INTELLIGENCE

The future of HTM extends beyond cybersecurity. By connecting CMMS platforms, cybersecurity tools, network discovery solutions, EMR systems, and asset management platforms into a unified ecosystem, organizations can transform disconnected information into actionable intelligence.

Instead of simply identifying vulnerabilities, healthcare organizations can begin answering strategic questions and begin the shift from a reactive discipline to a strategic operational capability in order to fortify their cybersecurity readiness.

Artificial Intelligence (AI) will undoubtedly play an increasing role in HTM, but AI is only as effective as the quality of the data behind it.

Organizations that invest today in connected technology ecosystems, standardized asset data, strong identity management, and modern cybersecurity controls will be best positioned to leverage AI in the future.

Securing the biomedical network is no longer just an IT initiative. It is both a patient safety and an operational excellence initiative—and, increasingly, a competitive advantage. ●

By the Numbers

62% of healthcare leaders surveyed by HIMSS Market Insights rated their inability to protect unpatchable or agentless medical devices as a critical or significant limitation in their organization's medical device security strategy.

*The Implementation Paradox—HIMSS & Elisity Healthcare Microsegmentation Survey on Medical Device Security, March 2026



Photo credit: ID 176619643 © Patrik Slezak | Dreamstime.com

HTM WORKFLOW TWEAKS TO SECURE DEVICES

From checking passwords to verifying software versions, routine maintenance gives HTM teams opportunities to strengthen medical device cyber-resilience.



Phil Englert is vice president of medical device security at Health-ISAC, where he works with medical device manufacturers to enhance privacy and security and coordinates with health delivery organizations to ensure implementation is practical and achievable.

By Phil Englert, VP Medical Device Security, Health-ISAC

Medical device cybersecurity is often discussed in terms of threats, vulnerabilities, and technical controls, but for healthcare technology management (HTM) professionals, the conversation is really about something far more familiar: maintaining the reliability, safety, and performance of the devices clinicians depend on every day.

Preventive maintenance helps ensure equipment functions as intended. Cybersecurity activities help ensure those same devices remain trustworthy, available, and safe for patient care. Cyber-resilience should not sit outside normal HTM workflows. It should be incorporated into the routine activities HTM teams already perform to keep medical devices operating safely throughout their lifecycle.

During a scheduled preventive maintenance inspection, technicians inspect physical components, verify calibration, and review device performance. That same visit provides an oppor-

tunity to validate cybersecurity controls that support the device's safe operation.

THE CYBERSECURITY CHECKUP

Routine maintenance offers a number of opportunities to incorporate these cybersecurity checks.

Consider an infusion pump. During a routine preventive maintenance check, technicians verify delivery volumes and alarm functionality and inspect mechanical components. That same workflow can include rotating passwords, confirming software versions, and confirming that default credentials have not been reintroduced. These actions require a few additional minutes but can significantly reduce the likelihood of unauthorized access to the device.

Ultrasound systems are another example. Many ultrasound machines temporarily store images and patient data locally even after the studies are transferred to the picture archiving and communication system. During routine maintenance, HTM personnel can verify that completed studies have been successfully transferred and that residual patient data is removed from local storage. In addition to helping protect patient information, this practice reduces unnecessary data accumulation and improves overall device hygiene.

Ventilators offer another example. During preventive maintenance, technicians frequently review device settings and operational logs. This can be expanded to include verification that unnecessary services remain disabled. If a service was temporarily enabled for troubleshooting or software support, HTM teams can confirm it has been properly turned off once the work is complete. Limiting unnecessary services reduces the device's attack surface while having little impact on day-to-day maintenance activities.

The same approach applies to anesthesia machines. During routine inspections, technicians can verify operating system versions, review available manufacturer updates, and confirm antivirus or application control mechanisms remain operational if those technologies are supported by the device manufacturer. These checks can become as routine as inspecting batteries, testing alarms, or evaluating gas delivery performance.

Imaging systems such as CT scanners, MRI scanners, and digital radiography units often contain complex networked components that interact with multiple clinical systems. During maintenance activities, technicians can verify proper communication with authorized systems while confirming that unnecessary external connections have not been established. Reviewing configuration settings, validating approved network paths, and checking that remote access controls remain properly configured can all be incorporated into existing service workflows.

MAINTAINING ACCURATE DEVICE INVENTORIES

Cyber-resilience also depends on maintaining accurate device inventories. HTM departments have long recognized the importance of tracking medical equipment throughout its lifecycle. Today, inventory records should also include cybersecurity-relevant information such as software versions, operating systems, network connectivity status, supported security features, and patch status where applicable. Maintaining this information helps organizations quickly assess exposure when new vulnerabilities are identified and supports more efficient remediation efforts.

Another valuable practice is the routine review of device configurations. Medical devices often remain in service for many years and undergo software updates, repairs, network changes, or clinical workflow modifications. Small configuration changes can accumulate over time and move a device away from its approved baseline. Periodic validation of security settings helps ensure devices remain configured as intended. For HTM professionals, this is an extension of the quality and performance verification activities they already perform.

"CYBER-RESILIENCE SHOULD NOT SIT OUTSIDE NORMAL HTM WORKFLOWS. IT SHOULD BE INCORPORATED INTO THE ROUTINE ACTIVITIES HTM TEAMS ALREADY PERFORM TO KEEP MEDICAL DEVICES OPERATING SAFELY THROUGHOUT THEIR LIFECYCLE."

A FUNDAMENTAL MAINTENANCE DISCIPLINE

HTM leaders did not hire a "pump maintenance department," a "ventilator maintenance department," and a "monitor maintenance department." Biomedical technicians developed the skills to incorporate maintenance of these devices into their normal workflows. Medical device cybersecurity should evolve in the same way.

Every HTM technician should be capable of performing basic cybersecurity maintenance activities on the devices they service. These activities should not be treated as separate workflows, although they will take additional time to perform.

Maturing programs can consist of cybersecurity-aware technicians, a few HTM cyber champions, and a small number of dedicated medical device security specialists. By incorporating basic cybersecurity activities into routine device maintenance, HTM teams can embed cyber-resilience into normal workflows while improving the security and reliability of the technologies clinicians depend on. ●

Did You Know?

A ransomware attack on a medical device manufacturer's cloud services disrupted cancer treatment at more than 170 healthcare facilities, according to a 2026 MITRE report examining emerging medical device cybersecurity risks.

*MITRE, Cybersecurity Risk Analysis for Medical Devices in the Era of Evolving Technologies, April 2026



ID 49998455 | Blood © Sudok1 | Dreamstime.com

YOU CAN'T PATCH EVERYTHING, SO OWN THE LIST THAT DECIDES WHAT GETS FIXED FIRST

Hospitals can't address every medical device vulnerability at once, making clear ownership of the priority list—and HTM's role in shaping it—critical.

By Shankar Somasundaram

When a vulnerability report comes in, there might be a few hundred threats flagged "critical." There's no path to resolving most of them this quarter (nor the one after it). No one in clinical engineering needs that scenario explained to them. Particularly as AI-accelerated vulnerabilities increase the stakes and the velocity, what can hospitals do?

Connected device/equipment security in hospitals has always been trickier than that of most other industries. A workstation might get patched overnight and rebooted before first shift, while an infusion pump running firmware that the manufacturer walked away from years ago does not.

Or, a CT scanner with a vulnerability that should otherwise be pulled offline keeps on scanning because radiology is already running behind. Scale complicates things, and with the average hospital now operating a couple dozen connected devices per patient bed, a large healthcare system can have hundreds of thousands of networked assets live at a time. All this while hospital cybersecurity draws somewhere between 4% and 7% of hospital IT budgets.

Then there's the question of who turns the proverbial wrench. Most medical equipment sits under manufacturer service agreements and regulatory constraints that keep IT from pushing updates on its own, so when fixes exist, applying them generally lands with clinical engineering. Often, healthcare technology management (HTM) absorbs the consequences of the priority order whether or not HTM had a hand in setting it.



Shankar Somasundaram is the CEO of Asimily, a cyber asset and exposure management platform. Previously, he worked on IoT analytics and security solutions at Symantec, where he helped lead the company's enterprise IoT product management.

The change needs to come with vulnerability

prioritization. Prioritization is the work, not the fallback position. Healthcare systems need to figure out who makes the call and understand what they know the moment they make it.

HOW THAT CALL GETS MADE TODAY

We recently surveyed North American hospital CISOs about decision-making around connected device vulnerability remediation. Twenty-two percent described some blend of vendor alerts, CVSS scoring (which is a whole other issue), and whatever they happen to know about how a device gets used. Another 18% run a manual review. Fifteen percent said they have no clear process in place (I credit them for the honesty because the real figure is almost certainly higher). Put those last two groups together and roughly a third of hospital security programs run without a repeatable way to decide what gets touched first.

The problem with vendor alerts is they often arrive late—and usually by design. There is a "patient zero" hospital out there somewhere well before a manufacturer issues their broader notification, and your facility may have been sitting inside that window for months. CVSS scores, meanwhile, put numbers to a severity in the abstract, with no awareness of your network whatsoever: A 9.8 on a device behind real isolation can be all but irrelevant in practice, while a 6.1 on a workstation with a clean path into your imaging archive probably deserves somebody's attention, right now.

TWO HALVES OF ONE DECISION

A truly defensible risk prioritization strategy requires two kinds of knowledge, and neither clinical engineering nor security holds both. Clinical engineering generally understands which devices are load-bearing for care delivery and which are effectively spares, where a device physically travels, what a two-hour outage does to the schedule, and which vendor is supposed to show up when you call. Security must know where a flaw is reachable from where the equipment sits, what the device genuinely communicates with, and how far somebody could move laterally after landing on it.

Nicholas Dybvig, assistant vice president of information security at Ardent Health, put it to me as, "A list built from either side alone is a guess dressed up as a priority order. Clinical engineering knows what the device is and what happens to patient care if a device goes down. Security knows what happens to the network if it's compromised. If you leave either one out of the room, the priority order isn't representing true risk."

WHEN YOU CANNOT PATCH, YOU CONTAIN

Most of the fleet will never be patched on a normal cadence. That puts the weight on a containment strategy, and thus clear network segmentation becomes critical. In no hospital should a compromised cardiac monitor have a network route into the EMR. No HVAC controller should reach anything financial. But without network segmentation, this is exactly what happens.

Segmentation projects stall anyway, but the reasons have very little to do with networking skill. Traditional access control reduces a device to an IP address and a MAC address, which reveals next-to-nothing about what the equipment is or what it needs to reach in order to do its job. Without that context, broad policies are written where nothing "breaks," but not much risk goes away either.

I see the same split showing up in network policy structure, where a policy that looks conservative on a whiteboard can still strand a device in the middle of a procedure, and the person who sees that coming is the biomed who supports it.

This (fixable) industry gap in segmentation orchestration is where we have put much of our effort at Asimily. Device intelligence that gets translated into policy can be pushed into a hospital's existing network access control, so what gets enforced reflects observed behavior instead of a best guess. Whether any of it survives contact with the floor still comes down to people, though, and specifically to clinical engineering reviewing a proposed policy before it goes live.

DON'T FUMBLE THE HANDOFF

Even with the right technology strategy, the handoff can make or break success. Ownership of connected equipment tends to get passed informally between departments until it lands with somebody who lacks the authority to act on it, or acts incompletely. Then you might get a third-party technician reconfiguring a machine during a service call without telling anyone.

Weeks later, security finds out secondhand or via an audit, if at all.

Closing the gap requires a live picture of the fleet that both groups are willing to work from. A spreadsheet accurate on the day somebody built it simply does not get you there. Once security and HTM read the same inventory and the same risk ranking, the handoff is no longer contingent on whether anyone remembered to send an email.

HTM teams get described as a stakeholder in these conversations, someone security ought to consult. I'd argue that framing sells the position short, and it lets clinical engineering leaders off the hook a little as well. You are the one scheduling the downtime and sitting on hold with the manufacturer (and, least appealing of all, explaining to a department head why their equipment is unavailable at the moment). The list becomes your problem the moment it lands, which is reason enough to be in the room where it gets built, well before it does. ●

Did You Know?

Health-ISAC notes that only a small subset of known vulnerabilities are actively exploited in real-world attacks and cautions that treating all vulnerabilities equally can dilute focus and obscure actual risk.

*Health-ISAC's From Metrics to Meaning: Transforming Medical Device Cybersecurity into a Strategic Risk Narration white paper, August 2026



Photo credit: ID 267732515 © Yuri Arcurs | Dreamstime.com

THE RISE OF THE CYBER BIOMED

A new career path is taking shape inside HTM as employers and training programs formalize the biomed cybersecurity specialist role.

By Alyx Arnett

When Nadia Elkaissi, CHTM, joined the Department of Veterans Affairs (VA) as a biomedical engineer more than a decade ago, cybersecurity training was built into the job from day one. Her supervisor, she says, was a "cybersecurity guru" who made cybersecurity a core part of the team's training, and the VA's structure gave biomeds a formal role in the networking and security of medical devices.

That kind of on-ramp is still relatively rare, but it's becoming less so. As connected medical devices multiply and cyberattacks against health systems accelerate, a distinct career track is emerging inside healthcare technology management (HTM): the cyber biomed. These professionals combine medical device expertise with cybersecurity skills, and employers and colleges are beginning to formalize the roles and training programs that support that career path.

"The future of HTM cybersecurity will depend on professionals who can speak both languages—the language of technology and the language of patient care," says Christopher Falkner, CCE, senior director of digital strategy and cybersecurity for healthcare technology management at Sodexo US.

A ROLE THAT EMPLOYERS ARE BEGINNING TO DEFINE

Sodexo is among the employers hiring specifically for cybersecurity-focused HTM roles, including BMET cybersecurity specialists. The company has been developing its approach to medical device cybersecurity for more than a decade. Falkner says Sodexo identified the need for dedicated specialists as medical devices

Worth Knowing

Health-ISAC says medical device manufacturers should clearly define whether a device's operating system and other third-party software can be patched without manufacturer validation—also known as "patch at will." They should also document expected update methods, patch cadence, and maintenance windows.

*Health-ISAC's MedTech Security Baselines white paper, August 2026

became increasingly networked, and cybersecurity expanded beyond protecting electronic health information.

"Cybersecurity is a patient safety issue, not simply a data privacy issue," Falkner says. "That's why we believe cybersecurity is now an essential part of HTM and the care delivery paradigm."

Today, all 600-plus Sodexo HTM employees complete a six-week cybersecurity training program, while a smaller group of BMET cybersecurity specialists provides deeper, proactive expertise at client hospitals. Falkner describes the specialist role as the point where medical device expertise and cybersecurity risk mitigation converge.

"Unlike traditional IT infrastructure, medical devices often require hands-on remediation, careful assessment of clinical impact, and coordination with the OEM to validate that security fixes can be safely implemented," he says. "BMET cybersecurity specialists lead that process while coaching fellow BMETs on cybersecurity requirements, remediation, and device availability."

What sets these specialists apart, Falkner says, is their clinical fluency. "They understand the realities of working in ICUs, operating rooms, and other care environments where cybersecurity decisions can directly affect the care patients receive," he says.

WHAT THE WORK LOOKS LIKE DAY-TO-DAY

At the VA Central Office, Elkaissi serves as a biomedical engineer in the Medical Device Networking and Cybersecurity Division, where she oversees networking and cybersecurity for VA HTM and supports biomeds across the country.

Her work ranges from coordinating with IT on high-priority vulnerabilities to investigating medical devices following cyber incidents, reviewing access control lists, and overseeing nine work groups responsible for areas including firewalls, technology implementation, and standardized HTM policies.

The role requires close collaboration with IT, but Elkaissi says medical device knowledge changes how cybersecurity decisions are made. "IT has a more general role," she says. "However, they don't have the medical device aspect or knowledge. So that's the thing that differentiates us."

IT staff may understand the necessary security controls, Elkaissi says, but not whether those controls can safely be applied to a particular medical device. "They don't know what patches need to be installed on a medical device," she says. "They don't know how it applies, how it should be configured in the group policy."

For Elkaissi, one of the most interesting parts of the work is seeing what that connectivity can make possible. "Probably my favorite part is seeing how much you can gain from a medical device, not just a standalone medical device, but what opportunities it can provide if it's networked," she says.

BUILDING CYBER EXPERTISE FROM WITHIN

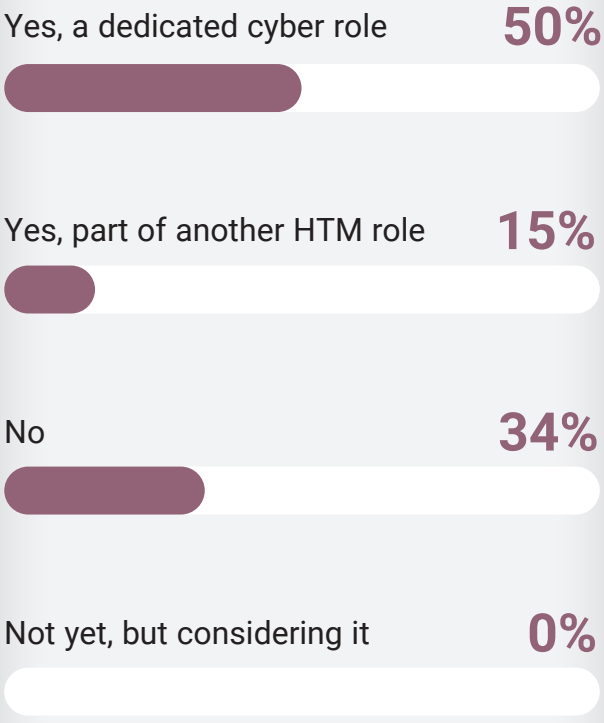
As the need for cybersecurity expertise grows within HTM, some organizations are developing those skills within their existing workforce.

At the VA, Elkaissi says biomeds receive extensive internal cybersecurity training as part of the job, supplemented by CompTIA training and vendor-led courses. Elkaissi has also pursued additional credentials to deepen her own IT and cybersecurity knowledge. She points to CompTIA Network+, Security+, and A+ as useful starting points for biomeds looking to build foundational knowledge of computers and networking. She says Network+ has also become a focus for VA trainees and interns, helping ensure they develop foundational networking knowledge as they enter the field.

24×7 Poll

Does Your HTM Department Have Someone Specifically Responsible for Medical Device Cybersecurity?

We polled 24×7 Magazine followers on LinkedIn about how their HTM departments are approaching medical device cybersecurity. Here's how 32 respondents answered:



Poll conducted on LinkedIn; 32 responses.
Results may not total 100% because of rounding.

Follow 24×7 Magazine on LinkedIn for more HTM polls and industry discussions.

The value of that foundational education is understanding the reasoning behind the work, Elkaissi says. Before learning the underlying concepts, she says, biomeds might be told to build an access control list without understanding what it was or why it was needed.

"At least having the knowledge of what we're supposed to be doing … is really important before you dive into the weeds," she says.

She is currently working toward the Cisco Certified Network Associate certification and plans to pursue the more advanced Certified Information Systems Security Professional (CISSP) next.

A COLLEGE PROGRAM BUILT AROUND THE ROLE

When John Schmidt, MA, vice president of operations at CBET, joined the college six years ago, he brought an IT background and began helping expand cybersecurity and networking education within its biomed programs. He saw parallels with consumer technology, where even appliance technicians increasingly need networking skills.

"When your Maytag repairman has to have a Network+ certification because your refrigerator and your stove and your washer dryer are all connecting to the internet, that kind of makes sense that inside of the healthcare organization we're in the same boat," he says.

Schmidt also saw more biomed departments moving from facilities management to IT, reinforcing the need for biomeds to understand networking. "There's only two departments at a hospital that own the medical Internet of Things—the IT department and the biomeds," Schmidt says. "Everybody else is a user. But biomeds own that equipment that's connected to the network, and IT owns that network."

That growing overlap between biomed and IT helped shape CBET's approach to its training programs. About four years ago, the college began developing the Biomedical Equipment Support Specialist (BESS) program, which incorporates cybersecurity and IT education into a broader biomed curriculum. The certificate and associate degree program includes electronics, biomedical equipment, and other core coursework alongside cybersecurity, networking, servers, and medical device integration. Students also learn how to bring that knowledge into areas such as procurement and change management, including identifying technology that may not be appropriate to connect to a hospital network. The associate degree can be completed in about 15 months on CBET's condensed schedule, Schmidt says.

For working biomeds seeking additional training rather than a degree, CBET offers shorter programs through its HTM Training Solutions, where the college works with employers to upskill existing staff. Its Biomedical Imaging and Information Systems (BIIS) course is a six-week program taught by an HTM cybersecurity professional over Zoom, paired with reading, quizzes, and discussion posts. Schmidt says more than 1,000 people have completed BIIS, which has been offered for five to six years. Sodexo was an early participant, with about 460 of its biomeds completing the program.

For biomeds looking specifically for healthcare networking training, CBET's Phase Connect covers DICOM, PACS, HL7, cybersecurity, and networking fundamentals through six weeks online followed by a four-day in-person lab.

SPEAKING THE SAME LANGUAGE

Additional education gives biomeds the technical knowledge to take on cybersecurity work, but Schmidt and Elkaissi say it also helps them communicate more effectively across biomedical, IT, and clinical teams. Schmidt refers to the divide between those groups as "the basement of Babylon."

"IT and biomeds and all those lab techs and all those niche organizations are all in the basement, and they all are for the same common goal of patient care. But they all talk a different language," he says. "What a biomed needs to do is overcome that. They need to learn how to speak to them and build trust, confidence, and camaraderie."

Elkaissi says that ability becomes especially important when HTM and IT are deciding how to address security risks on medical devices. IT may know which cybersecurity controls it would ordinarily apply to a networked system, but a biomed understands the equipment well enough to know whether those controls are appropriate for the device and its clinical use, she says.

She points to defibrillators as one example. She says IT personnel have pushed to install PIV cards on the devices, even though a defibrillator cannot support them. A biomed with cybersecurity training can assess the device within a risk framework and determine which security controls can safely be applied.That requires biomeds to understand IT well enough to communicate those needs, Elkaissi says.

"It's not just knowing the network, but it's kind of how to explain it to IT," she says, "so that everyone's on the same page."

At Sodexo, that combination of skills is built into the specialist role. Enterprise cybersecurity teams provide intelligence, monitoring, and analysis of emerging threats, but the onsite HTM cybersecurity specialists are responsible for translating that information into action at the medical device level. "These specialists don't just identify the vulnerability; they know the device in and out, as well as understanding the clinical environment and can drive the fix," Falkner says.

That can mean assessing the clinical impact of a vulnerability, working with an OEM to determine whether a security fix can be safely implemented, and coordinating with clinical teams before making changes to equipment. For Falkner, that hands-on role is critical.

"Medical device risk cannot be mitigated from a distance," he says.

WHERE THE CAREER IS HEADED

As cybersecurity becomes a larger part of managing connected medical devices, Falkner expects HTM to develop along two tracks: broader cybersecurity knowledge across the workforce and dedicated roles for those with deeper expertise. Cybersecurity fundamentals, he says, will increasingly become a core competency for HTM professionals, while "specialized hybrid roles will provide the deeper expertise needed to manage complex medical-device security risks."

CYBERSECURITY TRAINING AND CERTIFICATION OPTIONS FOR BIOMEDS

The certifications and training programs discussed by sources in this article offer a range of starting points for biomeds looking to build cybersecurity and IT expertise. While not an exhaustive list, the options below span foundational credentials, advanced certifications, and HTM-specific training.

Industry Certifications

CompTIA A+ — Covers foundational IT skills across hardware, networking, operating systems and security. Nadia Elkaissi recommends A+, along with Network+ and Security+, for biomeds looking to build a base of IT and networking knowledge.

CompTIA Network+ — Validates skills in areas including network connectivity, configuration, monitoring, troubleshooting and security hardening. Elkaissi recommends Network+ as a starting point for biomeds and says it has become a focus for trainees and interns at the VA.

CompTIA Security+ — Covers core cybersecurity skills, including securing networks, applications and devices and protecting the confidentiality, integrity and availability of data. Elkaissi recommends it as a foundational credential for biomeds developing cybersecurity expertise. CBET's John Schmidt also points to Security+ knowledge as an important baseline.

Cisco Certified Network Associate (CCNA) — Validates knowledge of network fundamentals and access, IP connectivity and services, and security fundamentals. Elkaissi is currently pursuing the CCNA as she continues to deepen her networking and cybersecurity expertise.

Certified Information Systems Security Professional (CISSP) — An advanced ISC2 certification focused on the ability to design, implement and manage a cybersecurity program. Elkaissi plans to pursue CISSP after completing her CCNA, while Sodexo supports its BMET cybersecurity specialists in pursuing the credential.

HTM-Specific Education and Training

Biomedical Equipment Support Specialist (BESS) — CBET's 30-credit certificate program prepares students to support the lifecycle management of networks, networked medical equipment and associated systems. Coursework incorporates cybersecurity, networking, servers and medical device integration alongside broader biomedical equipment education.

Biomedical Imaging and Information Systems (BIIS) — A six-week CBET course designed to establish an IT, information systems and cybersecurity foundation for biomedical equipment and imaging technicians. Schmidt says more than 1,000 people have completed the program.

Elkaissi also expects specialized roles to become more common, particularly as medical devices integrate more deeply with electronic health records, and cybersecurity becomes part of decisions throughout the equipment lifecycle—from procurement through implementation and sustainment. How those responsibilities are divided will continue to vary by organization, she says, particularly in health systems where HTM falls under IT.

Interest in additional training may already reflect the growing demand for cybersecurity and IT skills within HTM. Schmidt says CBET is seeing increased demand on its HTM Training Solutions side, describing employee upskilling, particularly around IT, as "increasing exponentially."

He also sees a generational shift underway as people who have spent their lives using connected technology enter HTM. "The kids nowadays that are starting, they're natives. They were born with the internet. They were raised on the internet," Schmidt says.

For biomeds who aren't planning to specialize in cybersecurity, Elkaissi still sees value in developing that knowledge. "Even if you're not a cybersecurity guru, or that's not your future, just having that as a knowledge base definitely will help your career," she says.

For those who do choose to specialize, Schmidt expects the skills that define today's cyber biomed to become increasingly central to HTM.

"The cyber biomed is going to be a requirement, not a nicety," he says. "The understanding and the adaptability of cyber into the medical device industry is going to be a basic requirement." ●

- Alyx Arnett is chief editor of 24x7 *Magazine.*

THE NEXT HEALTHCARE CYBERATTACK

MAY START WITH A TRUSTED VENDOR



Photo credit: ID 146060903 © Sasinparaksa | Dreamstime.com

Growing reliance on vendors, remote access, and connected technologies is expanding healthcare's cyber risk and putting greater emphasis on third-party oversight and continuity planning.

By William Hale, senior director of vCISO services at Magna5

Healthcare organizations are learning that a cyberattack does not have to begin inside their own network to affect patient care. In 2026, when third-party vendors CareCloud and Unlimited Technology Systems suffered cyberattacks, the damage went far beyond their own systems. Ultimately, these breaches exposed the sensitive health information of more than 7.5 million individuals, according to the US Department of Health and Human Services.



William Hale, senior director of vCISO Services at Magna5, provides executive cybersecurity leadership for highly regulated industries. He specializes in building actionable security programs, aligning risk management with business goals, and navigating complex compliance frameworks like HIPAA, HITECH, HITRUST, and NIST CSF.

Those incidents illustrate a larger problem: Healthcare organizations rely on a number of external vendors and third-party systems to support operations, all of which present potential cybersecurity vulnerabilities beyond their control. A breach within any one of these external systems can have serious consequences, compromising protected health information and disrupting essential healthcare operations.

For healthcare technology management (HTM) teams, the issue is no longer only whether a device, server, or network is secure. The critical questions are what each technology connects



to, who can access it, and what happens to clinical operations when one of those dependencies fails.

THE VENDOR ECOSYSTEM HAS BECOME PART OF THE CLINICAL ENVIRONMENT

Third-party risk is not new to healthcare, but its operational importance has changed.

According to Verizon's 2025 Data Breach Investigations Report, third-party involvement appeared in 30% of healthcare breaches analyzed, twice the share reported the previous year. This trend is significant as healthcare increasingly relies on technology environments that extend well beyond organizational boundaries.

A vendor may support an imaging platform. Another may maintain a connected medical device remotely. A cloud provider may host applications used for scheduling or documentation. A billing company may process revenue-critical information. A software vendor may maintain privileged access so technicians can troubleshoot systems without traveling on-site.

Each relationship creates another pathway into the healthcare environment.

The US Food and Drug Administration (FDA) reinforced this concern in its 2026 medical device cybersecurity guidance, noting that cyber incidents have rendered medical devices and hospital networks inoperable, potentially delaying diagnosis or treatment and causing patient harm. The agency also emphasizes that medical devices increasingly operate within larger ecosystems that include facility networks, other devices, software update servers, and external infrastructure.

That is an important distinction for HTM professionals. A device may be functioning exactly as designed and still become unavailable because another part of the technology chain has failed. Cybersecurity, therefore, has to be evaluated around the clinical workflow, not just the individual asset.

APPROVAL IS NOT THE SAME AS GOVERNANCE

Healthcare organizations conduct extensive due diligence before selecting technology vendors, but vendor approval is only the beginning. The greater risk often comes later.

Accounts remain active after projects end, privileged access is granted for troubleshooting and never reduced, and shared credentials survive employee turnover. Remote support tools stay connected continuously out of convenience, and vendors change subcontractors or infrastructure without security teams realizing their organization's exposure has changed.

A trusted vendor can also suffer its own breach. That is why third-party security should focus less on whether a vendor is considered trustworthy and more on what access the vendor has been given.

Healthcare organizations should be able to answer several basic questions:

- Which vendors can remotely access the environment?
- Which systems, devices, networks, and data can they reach?
- Is multi-factor authentication (MFA) required?
- Are privileges limited to what the vendor actually needs?
- Is access permanent, or can it be time-bound?
- How quickly can access be disabled during an incident or contract termination?

If those answers are unclear, the organization may have a visibility problem before it has a cybersecurity problem.

CONNECTED AND AI-ENABLED TECHNOLOGY ADDS ANOTHER LAYER

The growing use of artificial intelligence (AI) and connected medical technol-

Did You Know?

In Claroty Team82's analysis of more than 200 cyberattacks against cyber-physical systems, attackers often didn't need to exploit a software vulnerability at all. Many gained access through insecure protocols or weak, default, or missing credentials on internet-facing devices.

*Claroty Team82, Analyzing CPS Attack Trends, 2026

ogy makes these access questions more urgent. AI systems rarely operate in isolation. They connect to data repositories, application programming interfaces, cloud infrastructure, identity systems, clinical software, and operational workflows. Each integration creates another dependency and another identity that may require access.

IBM research found that 13% of surveyed organizations reported breaches involving AI models or applications, and 97% of those organizations lacked proper AI access controls.

The lesson for healthcare is not that AI should be avoided but that new technology should not be deployed without the same attention to identity, permissions, monitoring, vendor access, and supply-chain security that is applied to other critical systems.

For HTM teams, this can mean working more closely with information technology, cybersecurity, compliance, and clinical leadership before connected or AI-enabled technology becomes embedded into patient care workflows.

HEALTHCARE GROWTH CAN MULTIPLY INHERITED RISK

Vendor risk becomes even harder to manage as healthcare organizations acquire practices, consolidate locations, or standardize technology across multiple sites.

Each acquired location may bring legacy applications, unmanaged devices, old vendor accounts, shared credentials, remote access tools, and different cybersecurity practices. What was previously an isolated weakness can become a broader organizational exposure once environments are connected. Cybersecurity should therefore be part of integration planning, not post-acquisition cleanup.

Before connecting a new location, organizations should identify which systems and devices are being inherited, who maintains them, which vendors have access, whether MFA is enforced, how privileged accounts are managed, and whether backups and downtime procedures have been tested.

This is particularly important for technologies supporting direct patient care. A remote vendor connection created years ago for a single site may become much more consequential once that site joins a larger network.

HTM TEAMS NEED VISIBILITY AND CONTINUITY PLANS

Healthcare organizations cannot eliminate every third-party dependency, but they can reduce the risk those dependencies create. The first step is visibility. Organizations should maintain an inventory of vendors with access to medical devices, networks, applications, cloud platforms, patient information, or remote support tools. Vendors should then be prioritized based on the level of access they hold and the importance of the workflows they support. High-risk relationships deserve stronger controls.

- Limit privileged access. Vendors should receive only the permissions required for their work, and access should be removed when it is no longer necessary.
- Require strong authentication. MFA should be applied wherever remote or privileged access is possible.
- Monitor vendor activity. Authentication failures, unusual access patterns, policy violations, and privileged actions should not disappear into logs nobody reviews.
- Review access regularly. Vendor permissions should be reassessed as contracts, employees, technology, and clinical workflows change.
- Plan for vendor failure. Incident response and downtime planning should address what happens if a critical provider becomes unavailable. Teams should know who to contact, what evidence the vendor can provide, which workflows must continue, and how staff will operate while systems are restored.

"A DEVICE MAY BE FUNCTIONING EXACTLY AS DESIGNED AND STILL BECOME UNAVAILABLE BECAUSE ANOTHER PART OF THE TECHNOLOGY CHAIN HAS FAILED."

A strong cybersecurity program does more than prevent unauthorized access. It helps the organization continue operating when prevention fails.

CYBERSECURITY IS BECOMING A CARE CONTINUITY DISCIPLINE

HTM has always been concerned with availability, reliability, maintenance, and patient safety. Cybersecurity is increasingly inseparable from those responsibilities.

The FDA's medical device guidance makes that connection explicit. A cyber incident can make technology unavailable, delay treatment, and affect patient outcomes. As healthcare environments become more interconnected, those consequences may originate far outside the device or network where they ultimately appear.

The next healthcare cyber crisis may begin with a compromised vendor credential, an unmanaged remote support tool, an exposed software dependency, or a breach at a technology provider hundreds of miles away.

Healthcare organizations cannot control every external company they depend on. They can, however, control how much access those companies receive, how that access is monitored, and how prepared clinical teams are when a critical dependency becomes unavailable.

The goal is no longer simply to restore technology after an attack. It is to ensure that patients can continue moving safely through care while the organization responds. ●



Photo credit: ID 459993915 © Stockvectorwin | Dreamstime.com

REDUCING THE TIME FROM CHANGE TO RESPONSE

How to update cybersecurity assessments and controls between scheduled reviews.

By Kaarthick Subramanian, CISO and chief customer officer, Atlas Systems

A connected medical device could pass its scheduled maintenance check while its cybersecurity risk changes before the next review. A vulnerability could be found in a software component, a vendor could discontinue support, or a network change could increase exposure.

Even though the device continues to operate normally, its security assessment could be outdated. Healthcare technology management (HTM) teams need to connect those changes to devices in service and the people who will take action. Scheduled reviews act as a safety net; event-triggered reassessment can address changes that cannot wait.



Kaarthick Subramanian is chief customer officer and CISO at Atlas Systems. He built the company's security function. He holds the CISSP and has more than 20 years of experience leading global technology and services portfolios.

Continuous compliance means maintaining up-to-date risk assessments, controls, and supporting documentation. The goal is to reduce the time between a significant change and a verified response. An accurate record helps support compliance when it reflects the device's actual condition and the action taken.

AN ADVISORY CAN ALTER THE CLINICAL WORKFLOW

The US Food and Drug Administration's (FDA) January 2025 safety communication regarding Contec CMS8000 and relabeled Epsimed MN-120 patient monitors demonstrates how an external finding can necessitate reassessment of equipment currently in use. In July 2025, the FDA revised the communication to describe a software patch that, once applied, eliminates networking capability and restricts the devices to local monitoring.[1]

The ramifications of that response extend beyond the security record. The HTM team must determine whether care is dependent upon remote monitoring, coordinate with clinical users, and adhere to both the manufacturer's and the FDA's applicable instructions. A review remains incomplete until the operational consequences of the response have been confirmed.

The initial advisory, the manufacturer's response, and a subsequent mitigation may each change what the hospital needs to

do. As a result, advisory updates should remain integral to the response process until the related actions are completed.

SUPPORT DEADLINES SHOULD PROMPT DECISIONS PRIOR

Microsoft's Oct 14, 2025 end-of-support date for Windows 10 illustrates why lifecycle data must be included within a device's security record. The implications vary depending on the edition and support arrangement. Systems eligible for extended security updates may continue to receive security updates, whereas long-term servicing editions possess unique lifecycle dates.[2]

A record that simply states "Windows 10" cannot provide a reliable basis for a decision. HTM and security teams must know the edition and version of Windows 10, the medical device manufacturer's stance toward supporting the operating system, and whether any extended security update coverage applies. HTM and security teams should track platform support and support for the complete medical device separately.

An approaching deadline should compel a decision regarding whether to continue using the device, pursue manufacturer-supported upgrades, implement compensating controls, or replace the device. End-of-support status modifies the risk assessment; however, it does not, alone, constitute regulatory non-compliance. The record should explain the decision, who approved it, and when it will be re-evaluated.

COMPONENT VULNERABILITIES REQUIRE MORE THAN JUST A MODEL NUMBER

A device inventory identifies equipment. Responding to a software component advisory necessitates knowing which software versions exist in each device. A software bill of materials (SBOM) can facilitate establishing that relationship, provided that the SBOM accurately depicts the software deployed.

Section 524B of the Federal Food, Drug, and Cosmetic Act mandates an SBOM as a component of applicable premarket submissions for cyber devices. FDA's February 2026 cybersecurity guidance addresses these requirements and replaces its June 2025 guidance. Submission requirements do not signify that every legacy device in a hospital possesses an obtainable SBOM.[3,4]

Hospitals should request an SBOM and manufacturer disclosure statement for medical device security (MDS2) at the time of purchase, as well as provisions for receiving updated information. Link those documents to the relevant model and software release and then to individual assets. A general classification such as "infusion pumps" assists in assigning oversight but is inadequate for determining which units an advisory affects.

If software information is unattainable, document the gap and the manufacturer's response. Component matching should initiate an assessment of applicability and exposure, followed by a decision concerning action. Component matching should not be regarded as conclusive evidence that every matched device is vulnerable.

VISIBILITY MUST LEAD TO ACTION

Claroty's 2025 healthcare exposure study indicated devices containing known exploited vulnerabilities tied to ransomware and insecure internet connectivity were identified in 89% of the 351 healthcare organizations evaluated.[5]

Upon identifying an exposure, the response should link the advisory to affected assets, evaluate clinical ramifications and network exposure, designate an accountable owner, and establish a deadline commensurate with the risk. Completion requires documentation verifying that the action succeeded. For instance, following limiting a device's network communications, verify that the limitation is effective and that all necessary monitoring and clinical interfaces continue to function.

If remediation is postponed, document why postponement occurred, interim controls utilized, and subsequent review date. Acceptance of residual risk should emanate from the organization's designated risk acceptance authority, with clinical input where patient care is impacted. The individual maintaining the device record should not automatically be responsible for accepting that risk.

This methodology aligns with US Department of Health and Human Services guidance describing HIPAA risk analysis as an ongoing activity. Organizations must analyze changes affecting electronically protected health information and modify their protective measures accordingly. Hospitals need not await new rules to make reassessment an integral aspect of routine operations.[6]

CREATE A RECORD SUPPORTING THE NEXT DECISION

The device record should aggregate information usable by HTM, IT, security, and clinical teams. At minimum, the record should designate:

- The specific asset, model, location, clinical application, and accountable owner.
- The operating system employed by the asset, its firmware, applicable software versions, and manufacturer and platform support dates.
- The network location of the asset, its authorized communications, and its reliance upon dependencies such as remote monitoring or an electronic health record interface.
- The relevant SBOM and MDS2 (including versions/dates/known information gaps).
- Existing controls, verification evidence/dates of verification/open advisories/outstanding decisions.

Did You Know?

FDA recommends that manufacturers provide SBOM information to device users in a machine-readable format and keep it updated throughout the device's life cycle.

*FDA, Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, February 2026

Security verification dates should coexist with historical inspection/maintenance data. Both are required. Additionally, earlier decisions should be retained in order for the hospital to justify what was known at a given point in time and why a particular action was taken.

A common record does not require each team to use a similar application. It does mandate consistent asset identifiers, clearly defined responsibilities for each field within the record, and a method for resolving conflicting information. A named owner coordinates responses; HTM/security/clinical teams continue to contribute their respective areas of expertise.

INITIATE WITH A MANAGEABLE SUBSET OF DEVICES

Begin with a subset of devices selected based upon clinical significance/exposure (ie, a subset of connected monitors/imaging systems). Confirm deployed versions/support dates for each device; reconcile relevant inventories; identify individuals who will evaluate/approve changes.

Route manufacturer notifications/FDA communications/relevant vulnerability advisories through an established workflow (ie, existing maintenance system) if it supports cybersecurity triage or urgent escalation. Initiate review whenever software or connectivity changes occur following relevant third-party service prior to support deadlines. Conduct periodic checks to detect missed events or incomplete information.

Measure time required to identify affected assets, evaluate an advisory, and confirm remediation (grouped by risk priority). Track initial containment separately from permanent remediation, overdue actions, and exceptions awaiting review. Rapid evaluation is beneficial only if it results in timely action addressing exposure.

Hospitals should be capable of demonstrating which devices were affected, what action was taken, and how results were verified. When clinical teams can verify that patient care requirements are satisfied, security teams can demonstrate intended controls functioned effectively. Then the record provides verification of successful completion of response. ●

REFERENCES

1. US Food & Drug Administration. Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec & Epsimed. Safety Communication. January 30, 2025; Revised 2025 July 2
2. Microsoft. Extended Security Updates Program for Windows 10
3. US Food & Drug Administration. Cybersecurity In Medical Devices Frequently Asked Questions
4. US Food & Drug Administration. Cybersecurity In Medical Devices Quality Management System Considerations and Content of Premarket Submissions. Final Guidance Document. 2026 February
5. Claroty's State of CPS Security Report Healthcare Exposures 2025
6. US Department of Health & Human Services. Guidance On Risk Analysis

Advertise with

24x7

The Premier Resource for Healthcare Technology Management

✔ Low Advertising Rates
✔ Trusted HTM Audience
✔ Premium Editorial Content
✔ Access to Measurable Performance & Engagement Metrics



Explore our advertising opportunities today:
solutions.medqor.com/24x7-magazine/



SAME EXPECTATIONS, DIFFERENT RESOURCES

The reality of rural clinical-system cybersecurity.

By Don Seven, CISM, SecurityX, CySA+

A cybersecurity vulnerability does not become less serious because it exists in a small rural hospital. The vulnerability may be identical to one found in a large health system, and the expectation to manage that risk should remain. What changes dramatically is the environment surrounding the response.

Who is available to investigate the vulnerability? Who owns the clinical system? Does the hospital have internal healthcare technology management (HTM) personnel? Is another system available if the affected equipment needs to be taken out of service? Does the manufacturer still support it? Most importantly, does the organization have the resources and authority necessary to implement the recommended remediation?

Through my work with clinical systems across healthcare organizations of very different sizes, I have seen how easily limited resources can be interpreted as a lack of concern or effort. In many cases, that conclusion is wrong. Rural hospitals often



Don L. Seven is a senior clinical systems security engineer whose work focuses on connected medical technology, vulnerability governance, manufacturer coordination, and collaboration among HTM, IT, cybersecurity, and clinical teams.



recognize their cybersecurity risks and want to address them. Their challenge is implementing the same fundamental cybersecurity functions with substantially different staffing, funding, equipment redundancy, and access to specialized expertise.

This is where cybersecurity begins to show its true colors as a business decision. The technical answer may be clear, but whether an organization can implement it may depend on available capital, clinical priorities, manufacturer support, staffing, and the operational consequences of taking a system out of service.

The standard should remain firm. The path toward meeting it, however, must account for the environment in which the work is actually being performed.

WHEN ANYTHING TECHNICAL BECOMES IT

One of the most consistent differences I have encountered in rural healthcare is the organizational structure surrounding clinical technology.

Larger health systems may have separate HTM, information technology, networking, information security, compliance, clinical engineering, and capital-planning resources. In many rural facilities I have worked with, there was no internal biomedical or HTM department at all.

In some cases, there was essentially a biomedical room available for outside contractors when they came onsite, but no internal HTM staff responsible for the clinical-equipment environment.

As a result, IT became the executor of many biomedical projects and planning activities simply because IT was the technical resource available inside the hospital.

The problem was not a lack of ability or effort from IT. The problem was attempting to manage clinical technology using a model designed primarily for conventional information technology.

A medical device may contain familiar components: a Windows operating system, network interface, IP address, database, or common network protocols. That does not make it equivalent to a workstation or server. Clinical systems introduce manufacturer restrictions, service relationships, validation requirements, patient-care dependencies, specialized maintenance requirements, and equipment lifecycles that traditional IT processes may not account for.

Changes must also be considered within the manufacturer-supported and validated configuration of the system. I have encountered a situation where a remediation altered the system's software or programming enough that the resulting configuration no longer reflected what, in that instance, had originally been presented to the US Food and Drug Administration for clearance or approval. In clinical technology, closing a cybersecurity vulnerability without considering those downstream consequences can create an entirely different problem.

IT may understand the vulnerability but lack authority to modify the manufacturer's configuration. A contracted biomedical provider may maintain the equipment but have little responsibility for enterprise cybersecurity risk. Clinical leadership may understand the consequences of downtime but not the technical exposure. The manufacturer may control the supported remediation path while having no responsibility for the hospital's broader risk-management decisions.

Everyone may be involved while no one completely owns the outcome.

THE SAME VULNERABILITY CAN CREATE A DIFFERENT DECISION

My perspective on these differences comes partly from having worked at both ends of the healthcare-resource spectrum, including experience within a health system encompassing approximately 4,700 beds, as well as much smaller rural facilities.

Large organizations are not automatically better at clinical cybersecurity. Additional departments can create additional handoffs, disagreements about ownership, and slower decision-making. I have encountered clinical systems without clearly established owners in larger environments as well.

By the Numbers

Healthcare cybersecurity risks identified through Fortified Health Security's assessments remained open for an average of 345 days.

*Fortified Health Security, 2026 Mid-Year Horizon Report: The State of Cybersecurity in Healthcare, 2026

What larger organizations generally have is more options.

There may be specialized personnel available to investigate a finding, greater equipment redundancy, established manufacturer relationships, dedicated cybersecurity tools, and more flexibility to coordinate downtime. Rural hospitals may be working with a much smaller group of people responsible for several overlapping technical functions.

That changes what a seemingly simple instruction means.

"Patch the system" sounds straightforward until the manufacturer has not approved the patch, the service agreement has expired, the clinical application requires an upgrade, or the system cannot be taken out of service without affecting patient care.

"Replace the system" sounds straightforward until the vulnerable equipment is still clinically functional and replacement requires capital the hospital does not currently have.

"Remove it from the network" sounds straightforward until connectivity is necessary for the clinical workflow.

The difference is not competence versus incompetence. It is the type of friction each environment must overcome.

LIMITED RESOURCES SHOULD NOT MEAN UNMANAGED RISK

Recognizing those constraints does not mean rural hospitals should receive a pass on cybersecurity. If a vulnerable clinical system cannot be immediately patched, upgraded, or replaced, the organization still has a responsibility to manage the risk.

The question becomes what can reasonably be done now.

That may mean obtaining manufacturer guidance, identifying an accountable system owner, restricting unnecessary network communications, applying compensating controls, increasing monitoring, documenting why direct remediation is unavailable, or establishing a replacement plan.

The appropriate response depends on the system and its clinical function. What matters is that the vulnerability does not simply disappear from organizational attention because the preferred remediation is unavailable.

This distinction is important when evaluating cybersecurity maturity.

There is a meaningful difference between an organization that does not know a vulnerable system exists and an organization that has identified the vulnerability, investigated its options, documented why immediate remediation is not possible, implemented reasonable controls, assigned responsibility, and established a plan for eventual resolution.

Both organizations may still have a vulnerable system. They are not managing the risk in the same way.

ASSESS RISK MANAGEMENT, NOT PURCHASING POWER

Regulators, accreditors, cybersecurity professionals, and healthcare leadership should not lower fundamental expectations because a hospital is rural. Patients and the clinical systems supporting their care deserve protection regardless of ZIP code.

At the same time, measuring cybersecurity maturity solely by whether every vulnerable system has been patched or replaced risks confusing purchasing power with risk management.

A more meaningful evaluation asks whether the organization knows what it owns, understands its exposure, has assigned responsibility, has sought manufacturer guidance when necessary, has implemented feasible controls, and has established a path toward remediation or replacement.

It should also ask whether leadership has provided the people, authority, and funding necessary to perform those functions.

For some rural organizations, external HTM, cybersecurity, or clinical-engineering support will be necessary. The specialized expertise required to manage modern connected clinical technology cannot reasonably exist internally at every small hospital.

Seeking that expertise should not be viewed as evidence of failure.

"LIMITED RESOURCES SHOULD NEVER BECOME AN EXCUSE FOR UNMANAGED RISK. THEY ALSO SHOULD NOT AUTOMATICALLY BE MISTAKEN FOR NEGLIGENCE."

Expecting a small IT department to simultaneously perform infrastructure management, cybersecurity, user support, medical device management, manufacturer coordination, compliance activities, and clinical-technology lifecycle planning may create the larger risk.

SAME STANDARD, DIFFERENT PATH

Rural and large health systems should ultimately be held to the same fundamental expectation: identify cybersecurity risk and manage it responsibly.

They will not always reach that outcome through the same staffing model, technology, budget, or timeline.

The strongest rural cybersecurity programs will not necessarily be those with the newest equipment or largest security platforms. They will be the organizations that understand what they own, establish who is responsible, recognize when clinical technology cannot be treated like conventional IT, document why a direct remediation is unavailable, implement reasonable controls, and keep unresolved risks moving toward a sustainable solution.

Limited resources should never become an excuse for unmanaged risk. They also should not automatically be mistaken for negligence.

The better question is whether the organization can demonstrate that the risk is known, owned, reasonably controlled, periodically reassessed, and moving toward resolution. ●



Photo credit: ID 151977154 | Blood © Kukotaekaterina | Dreamstime.com

INSIDE A MEDICAL DEVICE CYBER INCIDENT RESPONSE

A four-stage response framework shows how HTM, IT security, clinical leaders, and executives can coordinate when a cyber incident affects medical devices.

By Tamra Durfee, senior virtual chief information security officer

Recent high-profile cyberattacks on medical devices and manufacturers including Stryker, Medtronic, and Contec Medical Systems, among others, have placed a spotlight on medical device security risks. When I speak with healthcare CISOs and other security leaders about how to deal with this, inevitably, the conversation turns towards incident response plans.

One reason for this is because traditionally these plans focus on isolating networking equipment and impacted workstations, not quarantining lifesaving medical equipment. As the stakes of a healthcare cyber attack rise, healthcare institutions need to integrate their incident response (IR) plans to satisfy the needs of both IT security and clinical leaders. Closing that gap between those two teams starts with who's in the room when a device incident happens.



Tamra Durfee is senior virtual chief information security officer at Fortified Health Security. She brings more than 27 years of experience in information security, compliance, regulatory risk, strategy, innovation, and technology transformation, with the past decade focused on healthcare cybersecurity.

QUICK STAT: Health-ISAC found that medical devices were impacted in nearly 10% of health-related ransomware cases in 2025.

WHEN AN INCIDENT IS IDENTIFIED, THE RESPONSE TEAM ASSEMBLES

The incident responses I have been a part of are often a mixture of chaos and calm. More thoughtful preparation typically means calmer, better and faster decision-making. When an incident is identified, the response team assembles. A common response team is composed of four roles:

- Healthcare Technology Management (HTM) – asset identity, location, service status, and validation of return to service.
- IT security – detection, segmentation, forensic scope, and the network controls that substitute for taking a device down.
- Clinical leadership – whether the device comes out of service, what replaces it, and the downtime procedure for the unit affected.
- Executive sponsor – regulatory notification, patient and board communication, and the authority to spend during the event.

Going into the first meeting, it is essential that each person understands their areas of responsibility and what decisions they are entitled to make. When authority is vague, it can lead to tension and delays that cost money and risk patient/staff safety.

WHAT DOES RESPONSE TEAM READINESS LOOK LIKE?

A well-rehearsed response team has thought through critical questions such as whether patients need to be moved to another facility. If the incident is limited to administrative areas, perhaps not, but the team will have drilled the decision tree down to a simple if this happens, then do this rule. You want a read-and-react decision, not one debated.

Similarly, the IT security team would know to avoid the natural inclination to isolate and contain everything, out of consideration for their clinical partners.

Choices about what to isolate or shut down must be collaborative. The process for resolving conflicting opinions must be established (or agreed upon) in advance.

Device incidents resolve in four stages, and they run in sequence whether or not anyone has assigned them. Each stage has a different owner, and the time you lose is almost always lost in the handoff between owners.

QUICK STAT: 99% of healthcare organizations are managing Internet of Medical Things (IoMT) devices with known exploited vulnerabilities (KEVs), per Claroty's analysis of 2.25 million IoMT devices across 351 organizations.

STAGE 1: DETECTION AND TRIAGE

Medical device incidents often start with a network alert or unusual device activity. IT security can detect the issue, but HTM must quickly confirm the device, location, owner, and patient-care impact. This requires a strong working relationship between IT security and HTM before an incident occurs; working together for the first time during an active response is a disaster waiting to happen. Triage slows when inventory is incomplete or clinical status is unclear. The control is a current device inventory with owner, location, connectivity, and clinical service status documented before an incident occurs.

This is a bad time to be thinking about asset hygiene. Before incidents occur, IT security and HTM should be teaming up to ensure that devices that are not being used are taken offline, that working devices have the latest firmware and security updates, and that inventories are accurate.

STAGE 2: CONTAINMENT WITHOUT CLINICAL DISRUPTION

Containment usually means segmentation or revoked access, not powering down the device. IT security executes the action, but clinical leadership must approve anything that affects availability. Risk increases when a device supporting patient care is taken offline before an alternative is ready. The control is a pre-approved containment tier for devices in clinical use, so response becomes a quick confirmation rather than a negotiation.

In this stage, the value of tabletop "fire drills" shows up immediately because they can identify conflicts that can be resolved before an incident happens. It is normal for different department heads to have different priorities or professional disagreements, but you can't afford delay-inducing differences of opinion in the heat of the moment.

QUICK STAT: 96% of hospitals report running end-of-life operating systems or software with known vulnerabilities, according to Oliver Wyman.

STAGE 3: ERADICATION AND VENDOR COORDINATION

Eradication depends on the manufacturer for validated firmware, patch timelines, and return-to-service approval. Delays happen when there is no named vendor contact, support spins in a general queue, or contract terms do not define response expectations. Be sure your vendor contracts name escalation contacts with a 24/7 SLA. Navigating a large manufacturer call tree at 2 am during an active incident only to get passed from person to person is unacceptable.

STAGE 4: NOTIFICATION, RECOVERY, AND LESSONS

Recovery means restoring the device to its validated baseline and addressing any required notifications to regulators,

Worth Knowing

FDA maintains a dedicated email address for questions about medical device cybersecurity involving CDRH-regulated devices: CyberMed@fda.hhs.gov

the manufacturer, or affected patients. This stage is a success when the lessons learned result in operational change. This could be improved vendor coordination and interdepartmental communication, or even commitments to rehearse and update IR plans. My view is that we fail patients if the same issues occur again.

Just as continuous improvement is good for products, it is good for IR plans.

Your IR plan has to account for as many variables as it can. Some are people-oriented; others are related to technology. The stress during a real incident makes it nearly impossible to think about everything. This is why simulating an incident to work the bugs out is such an enormous success factor.

But rehearsal only works if the data behind it is accurate, which is its own kind of inventory management.

THREE IR PLAN TESTING TYPES

The best IT organizations are great at all kinds of inventory management. They keep data fresh, relevant, and accurate, whether it's software licenses, digital certificates, or access controls. The same is true with IR planning. You have to know where all your patient monitors are, that your decision trees are accurate, and so on.

The majority of IR response success happens before an incident, including audits, rehearsals, and ensuring your security infrastructure is optimized to identify vulnerabilities in an era of AI-based attacks. We advise three types of preparation programs:

"IT SECURITY CAN DETECT THE ISSUE, BUT HTM MUST QUICKLY CONFIRM THE DEVICE, LOCATION, OWNER, AND PATIENT-CARE IMPACT."

- IR Program – a device-inclusive plan with named escalation paths, monthly maturity scoring, and mobile access when your own systems are down.
- Tabletop exercise – run with HTM and clinical staff in the room, not just IT, because the decisions that stall a device incident are theirs.
- Vulnerability threat management – visibility into which connected devices carry KEVs, so the Stage 1 triage question is already answered.

Put those three together and the payoff shows up in the numbers. Anecdotally, we have found that organizations that are prepared and tested can see a 50-75% reduction in downtime costs, with recovery that runs two to four times faster.

Success is the result of a plan that's been tested before it's needed. ●

MEDQOR
MARKETING SOLUTIONS
24x7

Stop Measuring Clicks.
Start Identifying Buyer Intent.

Performance-Based Marketing Powered by Chronicle

24x7 is part of **Chronicle**, the only integrated healthcare business intelligence network serving Healthcare Technology Management professionals.

The Chronicle Solution:
Chronicle analyzes meaningful engagement with trusted clinical content into actionable buyer-intent signals, and helping marketers identify and prioritize higher-value prospects.

With 24x7's Performance-Based Marketing (PBM) campaigns, you pay only for introductions to qualified buyers (MQLs).

Learn more about MEDQOR's Performance-Based Marketing programs.

Schedule a conversation with
Joe Del Grosso
347-456-6019 | jdelgrosso@medqor.com

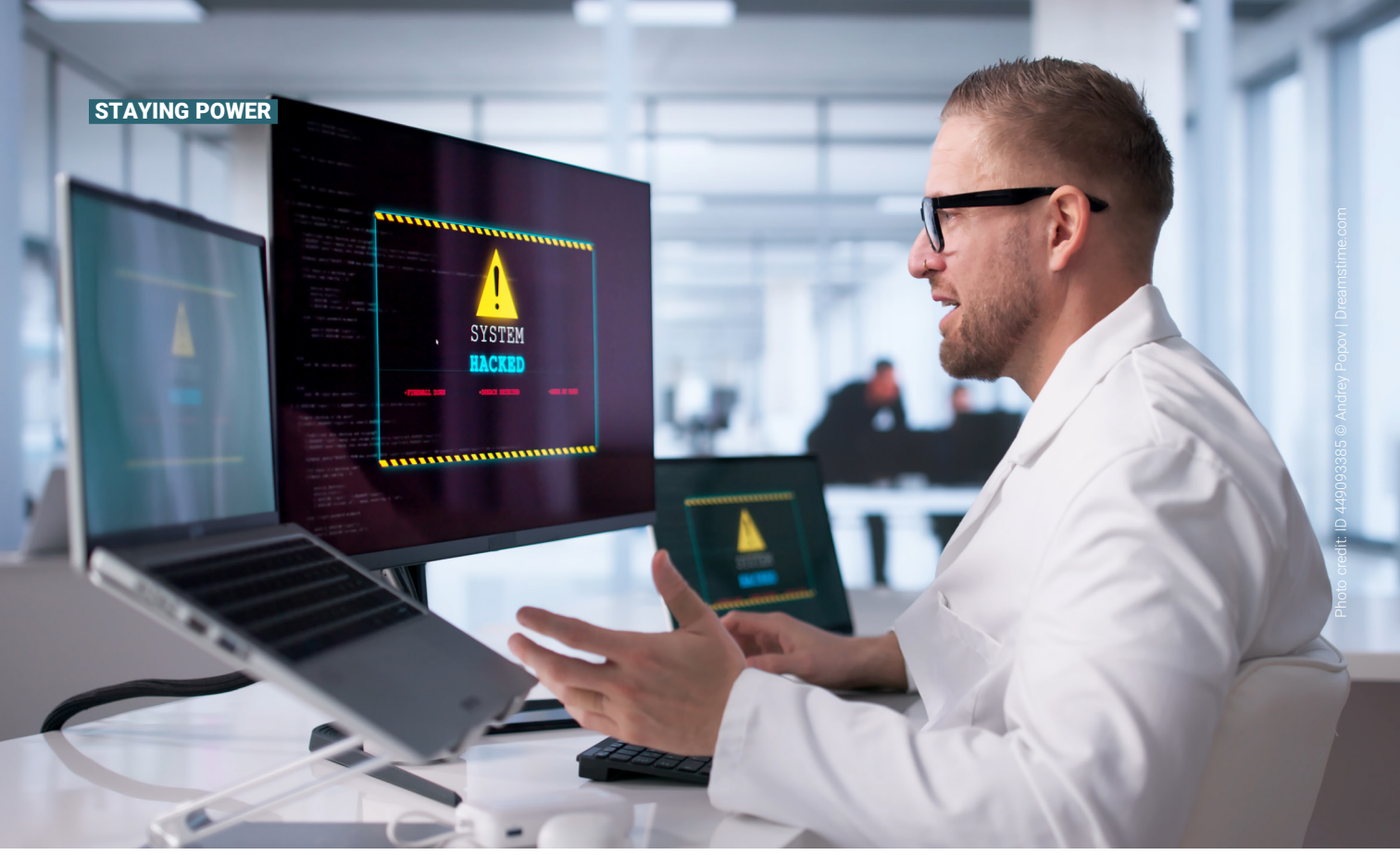


Photo credit: ID 449093385 © Andrey Popov | Dreamstime.com

CYBER RESILIENCE PROGRAM PUTS CLINICAL CONTINUITY IN HTM'S SIGHTS

Joint Commission and AHA leaders say hospitals should be prepared to sustain patient care for weeks when critical technology and connected medical equipment are unavailable.

By Alyx Arnett

When a cyberattack knocks a hospital into what industry leaders call "digital darkness," the impact can extend well beyond the electronic health record, according to William Walders, MHA, MBA, executive vice president and chief digital and information officer at Joint Commission.

Linear accelerators can become inaccessible. Infusion pumps can lose connections to centralized systems. In some cases, clinical staff have been locked in rooms when systems went down and doors failed shut, Walders says.

Those scenarios are shaping the second phase of the Cyber Resilience Readiness program, which Joint Commission and the American Hospital Association (AHA) rolled out as an expansion of the voluntary initiative first announced in May 2026.

"Our focus isn't around cyber maturity. Our focus isn't around helping people understand their cyber risk. It's truly to continue clinical operations," Walders says.

WHAT THE EXPANDED PROGRAM DOES

The Cyber Resilience Readiness program began in May with a free self-assessment designed to help hospitals evaluate their ability to maintain clinical operations during a prolonged technology outage. Organizations can use the questions internally or submit their results for expert review. The newly launched second phase adds fee-based advisory services from Joint Commission and

AHA, along with a formal Cyber Resilience Readiness certification managed by Joint Commission.

Walders says dozens of organizations have completed the assessment since its launch, while thousands more have viewed the questions. The assessment asks multidisciplinary teams to consider how patient care would continue during a technology outage.

"It's been eye-opening for these multidisciplinary teams to look at it not from the lens of IT, not from the lens of emergency management, not from the lens of operations, but truly on how to deliver clinical care safely," Walders says.

Organizations that want additional assistance can pursue advisory services from Joint Commission or AHA. Those seeking certification can move into a formal review intended to identify gaps as well as areas where an organization is already well prepared.

PLANNING FOR A 30-DAY OUTAGE

One of the challenges hospitals are being asked to consider is how they would maintain those clinical operations during a prolonged outage. According to Walders, the average period of "digital darkness" lasts 28 days. AHA recommends hospitals and health systems be prepared to sustain safe, high-quality care for at least 30 days without the technologies they normally rely on.

"They probably are comfortable surviving technology disruptions for 28 minutes, 28 hours, and then it starts to get hard when it's prolonged," he says.

Scott Gee, deputy national advisor for cybersecurity and risk at the AHA, says hospitals need operational plans for extended outages. Short-term workarounds, such as documenting on paper with the expectation that information can be entered into electronic systems once they return, become impractical when an outage stretches for weeks.

"That's not sustainable for 30 days, so we're encouraging people to build plans that they can execute and sustain for up to 30 days," says Gee.

Walders says prolonged downtime also raises questions about how hospitals prepare for medical equipment and other systems that may become disconnected. Organizations may need to consider whether to make the investment required to harden certain technologies or build a separate network that can continue functioning during an outage. For some, he says, the answer may be to accept that risk and plan for how operations will continue instead.

"For some organizations, the decision may be: 'We're not going to spend millions of dollars hardwiring every piece of clinical engineering equipment, from Da Vinci robots and linear accelerators to infant security systems and room controls. Instead, we'll build operational plans. We'll station staff at doors, bring radiologists onsite, and implement other manual processes that allow care to continue during an outage,'" Walders says.

28 DAYS

The average period of "digital darkness" following a cyberattack, according to Walders. Joint Commission and AHA recommend hospitals prepare to sustain care for at least 30 days without the technologies they normally rely on.

Making those decisions before an outage occurs reflects a shift Walders says he has seen during his 20 years in healthcare—from hoping a major technology outage won't happen to planning for the likelihood that it will.

For HTM teams, he says that planning should also accompany the adoption of increasingly connected and automated systems. "Every time somebody has a good idea around centralized monitoring, capacity management, [and] automation, [it] should come with the immediate plan on what happens when we don't have that," he says.

KEEPING CARE GOING IN DIGITAL DARKNESS

Ken Grubbs, DNP, MBA, RN, chief nursing executive and executive vice president of accreditation and certification operations at Joint Commission, says continuity planning also has to account for the clinical functions that cannot stop when technology becomes unavailable.

Hospitals still have to administer medications if automated dispensing cabinets are down, he says, and emergency department patients still need to be evaluated when imaging or laboratory systems are unavailable.

For Grubbs, preparedness means ensuring healthcare teams have a way to continue delivering that care during an outage.

"At the end of the day, we're all here for patients," Grubbs says. "If you think about the impact of a cyberattack, it impacts both those groups of individuals: the patients that are trying to receive care, and the healthcare team that wants to deliver that care." ●

- Alyx Arnett is chief editor of 24x7 Magazine.

Did You Know?

Medical device cybersecurity isn't limited to wireless or internet-connected capabilities. FDA's 2026 guidance also points to portable media, including USB drives and CDs, and the electronic exchange of device-related information when discussing the need for cybersecurity controls.

*FDA, Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions, February 2026

SCORECARD

HHS CYBER MODULE DRAWS STEADY UPTAKE FROM HEALTH SYSTEMS



Photo credit: ID 332370105 © Diok Klaisataporn | Dreamstime.com

Since launching in March, the RISC 2.0 cybersecurity module has helped hundreds of facilities benchmark their defenses—and revealed where healthcare still falls short.

By Alyx Arnett

When the Administration for Strategic Preparedness and Response (ASPR), a division of the US Department of Health and Human Services, added a cybersecurity module to its Risk Identification and Site Criticality (RISC) 2.0 Toolkit in March, the goal was to give healthcare and public health organizations a standards-based way to measure their cyber readiness alongside other hazards. Seven months later, ASPR says uptake has been steady, and the assessment is beginning to expose the vulnerabilities that healthcare organizations most often fail to address.

The module scores users against the Healthcare and Public Health Cybersecurity Performance Goals (CPGs) and the NIST Cybersecurity Framework 2.0, giving facilities a way to identify gaps, prioritize spending, and compare cyber risk against other threats already tracked in RISC. According to ASPR, 366 facilities have been added to the RISC Toolkit since the module launched, and 266 have completed the cybersecurity assessment—a sign, the agency says, of pent-up demand among healthcare technology management (HTM) and IT teams for a free, objective benchmarking tool.

"The idea for a dedicated cybersecurity module in our RISC 2.0 platform came from listening to those on the ground in our healthcare and public health systems on what they truly needed," an ASPR spokesperson tells *24x7*. "Recently, cyberattacks have consistently been ranking as a top threat of concern for our healthcare and public health sector."

WHERE ORGANIZATIONS ARE FALLING SHORT

Early data from completed assessments points to a consistent pattern of weak spots. ASPR says the top vulnerability-tackling tactics that healthcare organizations struggle with most, from highest to lowest, are network segmentation, third-party incident reporting, third-party vulnerability disclosure, and vendor and supplier cyber requirements.

Network segmentation—separating critical assets to minimize lateral movement within an environment by threat actors—tops the list. The other three all center on managing risk introduced by outside parties, an area of particular relevance to HTM teams that oversee connected medical devices sourced from a wide range of vendors.

"A healthcare facility is only as cyber secure as their weakest vendor or connected device," the spokesperson says.

A TIERED APPROACH FOR STRETCHED TEAMS

ASPR acknowledges that many organizations lack the staff or budget to address every finding at once. That's why the CPGs are divided into essential and enhanced goals. The essential tier is aimed at organizations with limited resources—"a rural healthcare clinic with only one part-time IT worker who doubles as front desk support, a small pharmacy just getting started," the spokesperson says.

The tiering is meant to give smaller facilities a defensible starting point rather than an all-or-nothing checklist.

"'Doing cybersecurity' is not a light switch that can be turned on," the spokesperson says. "Staying cyber secure is something you build up each day, and every step counts."

266

FACILITIES

have completed the RISC 2.0 cybersecurity assessment since the module launched in March, according to ASPR.

SIGNS OF RESILIENCE—AND PERSISTENT PRESSURE

Asked how the sector's overall posture looks in 2026, ASPR describes early but incomplete signs of progress. The spokesperson points to conversations with organizations that recovered more quickly from attacks because they had properly segmented backups, or resumed care faster because downtime procedure checklists told staff where to find items such as prescription pad lockbox keys.

Still, ASPR says the sector remains in what the spokesperson calls "an ongoing constant battle in this arms race." Looking ahead, the agency expects attacks to continue advancing in sophistication, with defenders needing to keep pace by adopting new technologies, including AI, and by building relationships with response partners before an incident occurs.

"'Hoping' it probably won't happen to you is not strategy," the spokesperson says. ●

Alyx Arnett is chief editor of 24×7 Magazine.

Did You Know?

Of Health-ISAC's 45 medical device advisories in 2025, 19 involved DICOM/PACS vulnerabilities.

*Health-ISAC, 2026 Global Health Sector Threat Landscape, January 2026

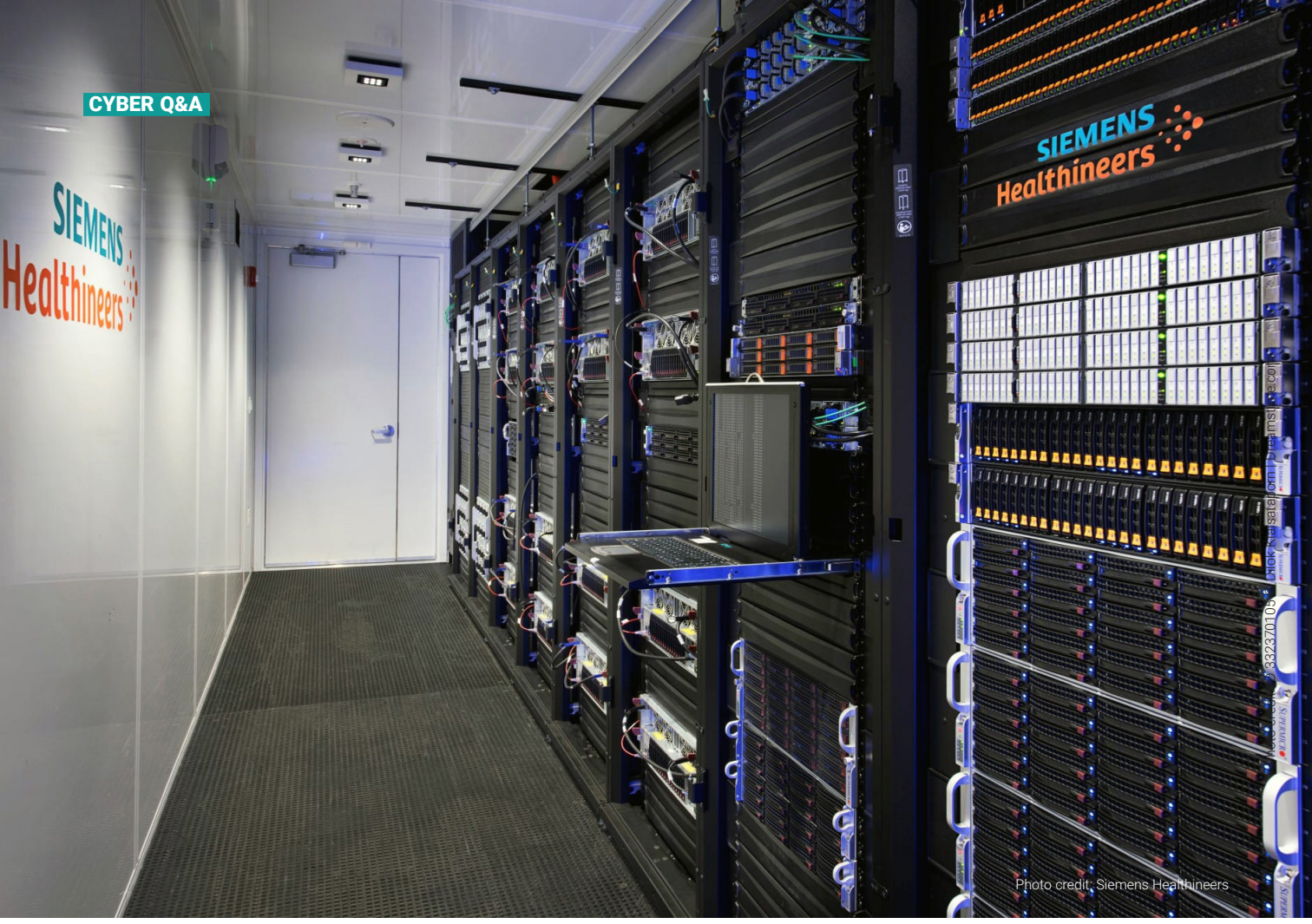


Photo credit: Siemens Healthineers

INSIDE SIEMENS HEALTHINEERS' $6.9M MEDICAL DEVICE CYBERSECURITY RESEARCH PROJECT

The ARPA-H-funded research explores how AI and large-scale simulation could help hospitals prioritize cybersecurity remediation while maintaining continuity of care.

By Alyx Arnett

Siemens Healthineers is taking aim at a familiar problem for hospital cybersecurity teams: how to address vulnerabilities in medical equipment without disrupting clinical operations. The company is researching whether artificial intelligence (AI) and large-scale simulation could help hospitals determine which vulnerabilities to address, when to address them, and what effect those decisions could have on patient care.

The company recently received a $6.9 million Phase I research project contract from the Advanced Research Projects Agency for Health (ARPA-H) to lead the Secure Healthcare Infrastructure Enhancement and Defense, or SHIELD, project. The effort is part of ARPA-H's Universal Patching and Remediation for Autonomous Defense program.

Working with industry and hospital partners, the SHIELD team plans to study how hospitals can better prioritize and time cybersecurity remediation while accounting



for the effects on equipment availability, clinical operations, and continuity of care. The research will use AI and exascale simulation to model interactions among medical devices, hospital operations, patients, and clinical staff.

24×7 spoke with Dorin Comaniciu, senior vice president of AI and digital innovation at Siemens Healthineers, about the problem SHIELD is designed to address, what the team plans to develop, and what the research could mean for hospitals and the HTM professionals responsible for connected medical equipment.

24x7: What problem did you see in hospitals that convinced you this research was needed?

Comaniciu: What we saw was that hospitals often know vulnerabilities exist, but determining what to fix first and how to do it without disrupting patient care is incredibly difficult. These decisions often span IT, HTM, and others, with each department working from different information and priorities.

Those silos slow down coordination and can leave critical vulnerabilities unresolved for months, even when the risk and fix are known. SHIELD helps bring that information together through a single pane of glass so healthcare organizations can understand the operational and clinical impact of remediation decisions, reduce cyber risk, and keep clinical care running smoothly.

24x7: What do you hope will exist at the end of the research?

Comaniciu: At the end of the research, we hope hospitals will have a practical platform that can identify vulnerabilities, model the impact of remediation options on patient care and operations, and guide organizations toward the safest path to reduce risk. This decision-support capability would reduce remediation timelines, improve cyber resilience, and help protect patient care while addressing cybersecurity risks.

24x7: What do you envision that platform being able to do?

Comaniciu: The goal is to give hospitals the information and confidence they need to make faster, better decisions. Over time, more of the analysis, testing, and remediation planning can be automated, while hospital leaders remain in control of whether and how changes are deployed. In simple terms, we want hospitals to move from reactive to proactive by understanding risk and acting before patient care is affected.

24x7: How are the hospital partners shaping what you're developing?

Comaniciu: Our hospital partners are essential because they provide real-world insight into how clinical workflows, staffing constraints, maintenance processes, and patient care requirements influence cybersecurity decisions. What we're learning is that cybersecurity decisions in hospitals are rarely just technical decisions. Every remediation can have downstream impacts on clinical operations, equipment availability, and patient care. By working directly with hospitals, we can better understand those tradeoffs so SHIELD will work in actual hospital environments.

24x7: What are the major hurdles to moving from today's largely manual processes toward autonomous remediation?

Comaniciu: The biggest challenge is the complexity of hospital environments. Hospitals may have thousands of connected devices from different vendors, legacy systems, and limited visibility into how those systems interact. Creating accurate digital representations of those environments and reliably predicting the effect of a remediation at scale is difficult on its own.

On top of that, hospitals must balance cybersecurity, system uptime, staffing constraints, clinical priorities, and patient safety every time they consider a change. SHIELD is focused on building an accurate operational twin of a hospital's clinical and IT operations, bringing all of this information together and leveraging the power of AI and exascale simulations to help organizations understand those tradeoffs in seconds so they can make faster, more informed decisions with confidence.

24x7: What could the research mean for hospitals?

Comaniciu: Hospitals will be able to make cybersecurity decisions in the context of patient care rather than in isolation. Today, vulnerability management is often driven by technical information alone, but hospitals have to consider how those decisions affect clinical workflows, equipment availability, staffing, and operations. SHIELD aims to provide that broader context, helping HTM professionals, cybersecurity teams, and hospital leaders understand not only where risk exists, but also the likely impact of different remediation choices. The result would be more informed decisions, faster remediation, and a stronger ability to reduce cyber risk while maintaining continuity of care.

24x7: What happens after Phase I?

Comaniciu: The longer-term vision is much bigger than helping a single hospital decide how to remediate a vulnerability. We envision a future where healthcare organizations can model how care is delivered across an entire region and understand how cyber events, equipment outages, or remediation decisions ripple through the broader healthcare ecosystem. If a critical system becomes unavailable at one hospital, what happens to patient flow, emergency services, specialty care, and neighboring facilities? How does a decision in one part of the system affect capacity and care delivery elsewhere?

The opportunity is to create a predictive environment that helps healthcare leaders understand those interdependencies, test scenarios before they occur, and make decisions that optimize resilience across the healthcare system as a whole by utilizing AI at scale. ●



24x7

WANT MORE?

Check out our digital edition at

24x7mag.com/magazine-archive/


OZARK
BIOMEDICAL
When It Comes To
CENTRIFUGES,
One Name Stands Out
YOUR SINGLE SOURCE FOR PARTS AND DEPOT REPAIR
StatSpin Express 2, 3, 4
We have a complete line of parts as well as service available.
Your Centrifuge Solutions Center
• Free Tech Support
• Depot Repair
• Flat Rate Repairs
• Re-manufactured Parts
• New Parts
• Exchanges
www.ozarkbiomedical.com
800-457-7576



CHAI'S PUSH TO BUILD HEALTHCARE'S FIRST PLAYBOOKS FOR FRONTIER AI CYBER RISK

A new work group is developing playbooks, expected by the end of the year, to help health systems respond to emerging AI cyber threats.

By Alyx Arnett

The time hospitals have to respond to a cyberattack could be shrinking dramatically as increasingly capable artificial intelligence (AI) models enter the equation. Cyberattack tasks that once unfolded over days or weeks could potentially happen in seconds, creating a problem that traditional cybersecurity processes—and human responders—may not be fast enough to address, says Coalition for Health AI (CHAI) CEO and co-founder Brian Anderson, MD.

Anderson points to Anthropic's Mythos-class models, a new generation of highly capable AI models designed to perform complex tasks with greater autonomy, including the public Fable variant released in June 2026. He says these models are changing the cybersecurity landscape by compressing attack timelines and expanding what bad actors could potentially do with PHI exfiltration and ransomware.

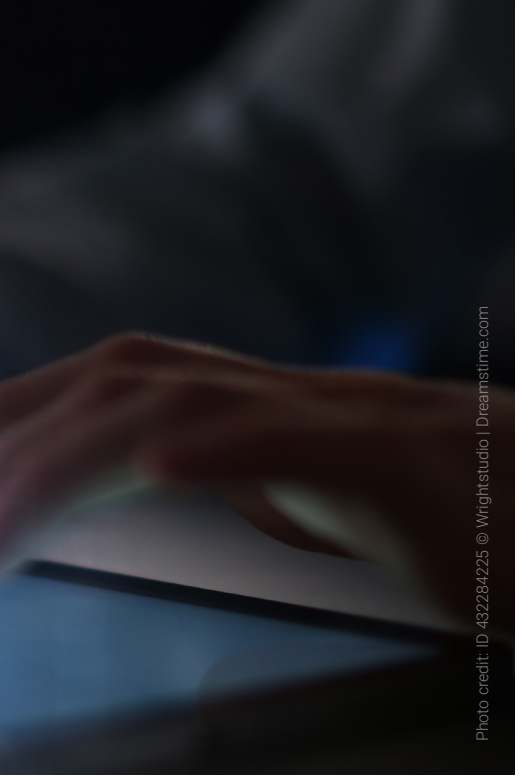
With the capability of these Mythos-class models ... no human can respond that quickly," he says.

Those emerging capabilities are part of what prompted CHAI to launch its new Health AI Cybersecurity Work Group. The nearly 100-member group is developing guidance aimed at helping health systems respond to threats posed by frontier AI models while also exploring how the technology can be used for cyber defense, with playbooks expected by the end of 2026.

Did You Know?

Even a medical device that doesn't contain AI may include software developed with the help of AI. MITRE warns that AI-generated code could introduce unusual bugs that are harder to detect and diagnose using security tools designed around established code patterns.

*MITRE, Cybersecurity Risk Analysis for Medical Devices in the Era of Evolving Technologies, April 2026



WHY HEALTHCARE NEEDS ITS OWN PLAYBOOK

The idea for the work group grew out of what CHAI saw as a gap in broader efforts to address the cybersecurity implications of advanced AI. Several initiatives are already bringing technology, infrastructure, and cybersecurity organizations together to explore how AI can be used to strengthen cyber defenses. Among them, Anthropic's Project Glasswing focuses on finding and fixing vulnerabilities in critical software, while OpenAI's Daybreak Defense Network works with cybersecurity companies and other partners to develop AI-powered defensive tools and workflows.

But Anderson says health system and payer leaders were concerned that healthcare and its particular operational challenges were not represented.

"There was a growing chorus ... within CHAI that were saying we need to have a health sector-specific effort that takes into consideration the unique things about the health sector," Anderson says.

To address that gap, CHAI brought together health systems, payers, and technology companies to develop guidance tailored to healthcare's needs. The goal is not simply to identify the risks posed by more capable AI models, but to get specific about how healthcare organizations could respond.

"No one has developed these kinds of playbooks yet," Anderson says. "We need to get to that level of technical specificity."

As an example, Anderson says the guidance could distinguish between the technical steps an organization might take with a Cisco router versus another type of router.

WHAT THE WORK GROUP IS BUILDING

The work group plans to develop a defensive playbook, an offensive playbook, and a frontier AI cyber risk assessment tool, among other resources. A leadership council will oversee the effort and work to ensure the resources reflect the threat levels hospitals and health systems are currently facing. The group is also exploring what it looks like to use AI itself as part of that defense. One area Anderson points to is agentic orchestration. As health systems deploy AI agents capable of carrying out multistep tasks, they will need ways to manage those agents' identities, permissions, and actions in real time.

"No human can do that," Anderson says. "We need AI tools that are actually monitoring the actions and the steps that these agents are taking."

Exposed API endpoints are a potential use case. Anderson says AI agents could monitor those connections for unauthorized access and respond by using tools, writing code, or denying permissions—allowing some defensive actions to happen at speeds a human analyst could not match.

> **"NO ONE HAS DEVELOPED THESE KINDS OF PLAYBOOKS YET. WE NEED TO GET TO THAT LEVEL OF TECHNICAL SPECIFICITY."**
> — Brian Anderson, MD, CEO and co-founder, CHAI

Some of those capabilities are already being developed. Anderson says some of the leading technology companies CHAI is working with had early access to Mythos through Project Glasswing and have been building tools and capabilities aimed at the needs of health systems and payers.

WHAT COMES NEXT

Once the playbooks are released, Anderson says the goal is for health systems to be able to use them to begin putting new defensive strategies into action with the teams and tools they already have.

CHAI also wants the guidance to be usable by hospitals without the resources of a large academic medical center and has included community health systems, safety-net clinics, and rural health clinics on the leadership council to ensure the guidance reflects the needs and constraints of smaller and lower-resource healthcare organizations.

"If we build a set of operational and defensive strategy playbooks that can only be implemented by the most well-resourced academic medical centers, this effort will be a failure," Anderson says.

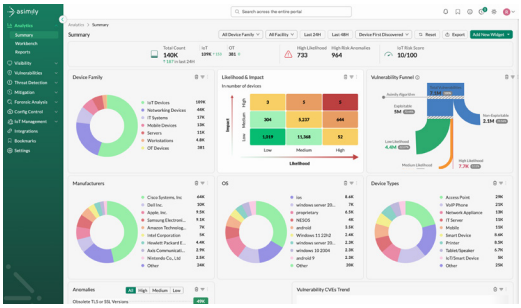
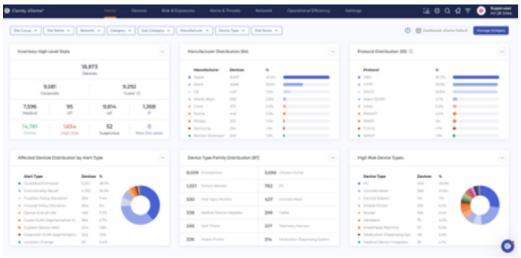
The finished materials will be publicly available, though CHAI plans to use a vetting process modeled on Health-ISAC's approach to releasing technical guidance to avoid providing bad actors with a roadmap.

In the meantime, Anderson encourages HTM teams to engage with the work in progress. Additional webinars are planned between now and December, when CHAI aims to have substantive materials ready to share around the Health-ISAC convention.

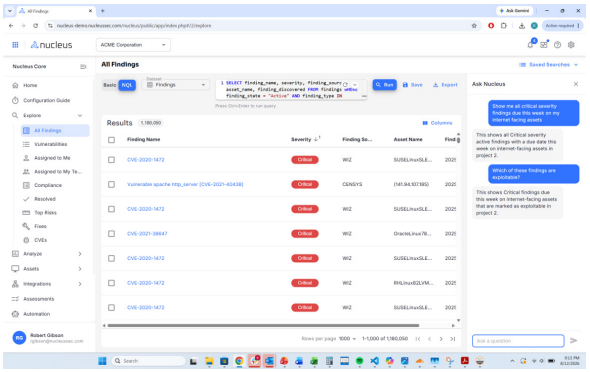
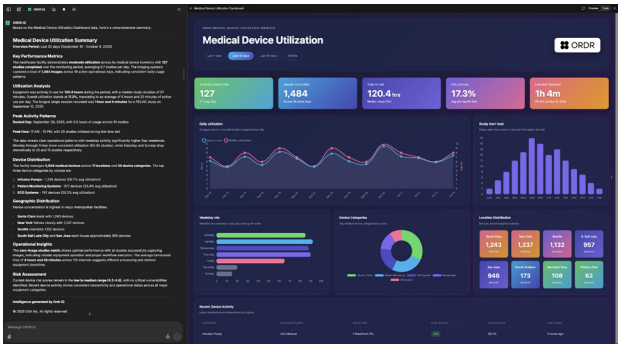
"This is all about sharing and developing insights that can only happen when we come together and develop those best practices," he says. ●

Alyx Arnett is chief editor of 24x7 Magazine.

COMPARISON GUIDE

Company name	Asimily	Claroty
Cybersecurity software	 Asimily	 Claroty xDome
Website	asimily.com	claroty.com/healthcare-cybersecurity/xdome-for-healthcare
Description	Asimily is the proactive cyber asset defenseplatform across your entire cyber asset attack surface: IoT, OT, IoMT, and IT. It closes the loop from risk intelligence to enforced policy, identifying the riskiest 1% of devices, prioritizing what matters with ATT&CK Analysis and orchestrating the segmentation and mitigation actions that contain exposures without disrupting clinical operations.	Claroty xDome is an AI-powered healthcare cybersecurity platform that protects all CPS in clinical environments, including IoMT, IoT, and OT. It provides the deepest visibility and broadest protection across asset inventory, exposure management, network security, threat detection, operational efficiency, and secure access.
Last major update	July 2026	2026
Introduced in the last update	Network Topology View, a graphical map of network traffic flows layered with Asimily's calculated risk posture	Claroty Claire, AI-powered CPS security agent for visibility, insights, remediation, and visibility orchestration for asset enrichment and DDoS detection.
Asset discovery method	Agentless discovery, deep packet inspection, active querying, agent-based discovery, integration with existing IT systems, cloud-based visibility	Passive network monitoring, active querying, integration with existing IT systems, cloud-based visibility, Claroty Edge
Risk scoring approach	ATT&CK Analysis for real exploitability, CVE-based scoring, contextual risk, patient safety/clinical impact considered, customizable risk scoring by facility, threat intelligence integration	CVE-based scoring, contextual risk, patient safety/clinical impact considered, customizable risk scoring by facility, threat intelligence integration, Risk scoring, KEV and EPSS scores, AI-enriched asset and risk context, prioritized exposure remediation with manufacturer required actions
Deployment model	Hybrid	SaaS (cloud-hosted)
Typical deployment time	<30 days	<30 days
Clinical/HTM workflow support	Supports biomed/HTM-specific workflows, provides device service history or utilization reports, enables collaboration between HTM and IT teams, generates work orders or service tickets	Supports biomed/HTM-specific workflows, provides device service history or utilization reports, enables collaboration between HTM and IT teams, generates work orders or service tickets
Pricing model	Annual subscription, per-bed pricing, tiered pricing	Annual subscription, per-device pricing, enterprise flat-rate pricing, tiered pricing
Typical annual cost	Dependent on unique hospital	Not provided

Information for this guide is based on data submitted by cybersecurity software marketers. *24×7* strives for accuracy in all data but cannot be held responsible for claims made by marketers. All cybersecurity software marketers get one listing at no charge. Advertisers are offered multiple listings. All cybersecurity software platforms may not be included. Email editor@24x7mag.com to be considered for the next update.

Nucleus Security	ORDR
	
Nucleus Security Platform	ORDR AI Protect Platform
nucleussec.com	ordr.net
Nucleus Security's platform unifies vulnerability data across tools, enriches it with real-world exploitation intelligence, and enables healthcare organizations to prioritize risk, prevent breaches, and accelerate secure, automated remediation workflows across clinical and IT environments. Nucleus Helix is the platform's AI engine for exposure management.	ORDR is the only purpose-built platform to help organizations see, know, and secure every connected device—from traditional servers and workstations to IoT, IoMT, and OT devices. Crunchbase competitors often specialize in one segment; ORDR provides a unified view across all device types.
August 2026	March 2026
New agentic capabilities combine vulnerability intelligence, exposure discovery, and AI-built autonomous workflows to help HTM security teams scale exposure management programs.	ORDR IQ, multi-agent AI orchestrator for end-to-end workflows, exposure risk to highlight risk based on compliance requirements
Integration with existing IT systems, cloud-based device visibility	Passive network monitoring, active querying, agent-based discovery, integration with existing IT systems, cloud-based visibility, log analysis
CVE-based scoring, contextual risk, external exposure, compliance scope, patient safety/clinical impact considered, customizable risk scoring by facility, threat intelligence integration including real-time exploitation, KEV, and EPSS	CVE-based scoring, contextual risk, patient safety/clinical impact considered, customizable risk scoring by facility, threat intelligence integration, connectivity, business context, exposure based on gaps/compliance
SaaS (cloud-hosted), on-premises	SaaS (cloud-hosted)
<30 days	<30 days
Generates work orders or service tickets	Supports biomed/HTM-specific workflows, provides device service history or utilization reports, enables collaboration between HTM and IT teams, generates work orders or service tickets
Annual subscription, per-device pricing, tiered pricing	Annual subscription, per-device pricing, per-bed pricing, tiered pricing, per employee
$40,000-<$1M	300 bed; ASP $150,000

SOUTHEASTERN
BIOMEDICAL INC
MEDICAL EQUIPMENT SALES AND SERVICE







BIOMEDS HELPING BIOMEDS™

Expert, cost effective on-site test equipment calibration and repair services

Our test equipment calibration service will:

- Eliminate shipping costs and damage
- Reduce downtime from weeks to hours
- Increase productivity

Our calibration management software will:

- Allow us to identify and notify you when your equipment is due for calibration
- Provide an online history of calibration and repair services performed on your test equipment

FLUKE Biomedical
Authorized Fluke Biomedical Service Center

CERTIFIED ISO 9001:2015 COMPANY

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17025
CALIBRATION LABORATORY

CONTACT US TODAY!

(828) 396-6010 | sebiomedical.com