KPMG

Navigating the next era of healthcare cyber risk

Six shifts redefining cyber risk: What payers and providers need to know to secure the enterprise

kpmg.com

Beyond the cyber status quo:
Healthcare's new threat matrix

For healthcare executives, cyber security can often feel like a permanent state of triage. The alarms sound, threat mitigations are deployed, leadership's dashboard toggles between red and green, and, inevitably, the cycle repeats. It's a familiar, business-critical routine.

But that familiarity can quickly become a vulnerability as cyber risks expand relentlessly and get ever more complex. You can execute today's playbook perfectly and still be completely unprepared for the emerging threats on the horizon. Data security remains a huge focus. But, as recent headlines demonstrate, hackers are increasingly able to inflict more immediate, catastrophic harm across a broader attack surface: freezing cash flow, ransoming the connected care continuum, manipulating clinical logic, and more.

Consider the speed of the macro shifts in motion. AI creates myriad new risks that existing cyber security rules never contemplated. Care is now more connected and digital—a massive win for patients, but a sprawling new target for bad actors. You have more vendors, your vendors have more vendors, and everyone's systems—and risks—are more interconnected than ever. Meanwhile, this expanding ecosystem is triggering more regulatory traffic. And even as AI is breaking the cyber template, quantum computing is looming, ready to rewrite the rules of encryption entirely.

The convergence of these forces is fundamentally redefining the concept of "secure healthcare." Security is no longer a static defensive perimeter, but a continually evolving, top-tier enterprise priority that must be embedded directly into the organization's clinical, financial, and operational mandates. Maintaining the status quo means actively accepting risks with potentially severe consequences.

Here's what healthcare leaders need to know about six structural shifts reshaping the cyber landscape—and the decisive actions required to stay ahead of the related risks.

WHAT THE DATA SAYS:

82% OF CEOS RATE CYBER CRIME AND CYBER INSECURITY AS THE TOP THREAT TO THEIR ORGANIZATION'S GROWTH AND PROSPERITY

2025 KPMG US CEO Outlook, October 2025

#1 Governing AI and the agentic workforce

AI is the most urgent catalyst forcing healthcare leaders to rethink their security posture. Yes, it's a paradigm-changing technology that can expand operational capacity, productivity, and growth. But it simultaneously exposes entirely new attack vectors and renders many traditional internal checks and balances obsolete.

What leaders need to know

The market is racing to adopt agentic AI. Unlike traditional automation, these non-human identities can orchestrate complex workflows and make decisions on behalf of clinicians and administrative staff. This expansion creates a massive new threat matrix. For example, there's the risk of "intent drift"—a scenario in which a compromised or hallucinating AI agent alters its programmed logic to execute unauthorized, potentially harmful tasks in the background. You are essentially giving these new digital "staffers" the keys to your clinical and financial systems without first creating a reliable way to monitor them.

The action plan

- **Establish an identity-first security model.** Organizations must build strict access management frameworks designed specifically for non-human agents. Security teams must inventory and govern these machine identities with the same rigor used to manage human employees.
- **Keep a human in the loop.** Leaders must maintain oversight to verify AI-generated clinical insights before they influence patient care. Unchecked AI outputs carry significant clinical and financial risks, making a human safety net essential for verifying accuracy and intent.
- **Build technical kill switches.** Your technology infrastructure must include the ability to immediately sever access and terminate a rogue agent the moment it deviates from its approved purpose.

WHAT THE DATA SAYS:

92% OF TECHNOLOGY LEADERS SAY MANAGING AI AGENTS WILL BE AN ESSENTIAL SKILL WITHIN THE NEXT FIVE YEARS

KPMG Global tech report 2026

#2 Securing the connected care continuum

Digital innovation is radically transforming how and where care is delivered. The traditional hospital network perimeter hasn't disappeared, but it is rapidly stretching to cover entirely new use cases. In its place is a sprawling web of connected devices that can track patients from the intensive care unit back to their living room.

What leaders need to know

Provider workflows—and the payer networks that reimburse them—now depend heavily on the Internet of Medical Things (IoMT). This includes everything from connected hospital beds and electrocardiogram machines to in-home glucose monitors. These devices constantly transmit data across internal and external networks, yet many lack the computing power required to run robust security controls. This vulnerability can have life-or-death implications, especially as hostile actors seek new ways to create disruption. A compromised IoMT device, for example, can quietly feed false readings directly into an electronic health record, triggering unnecessary and potentially dangerous clinical actions before a clinician realizes the data is tainted.

The action plan

- **Build a comprehensive device inventory.** You can't protect what you can't see. Organizations must establish a continuous, real-time inventory of all operational technology and connected medical devices operating both inside the hospital walls and in remote care settings.
- **Govern the flow of external data.** Providers can't secure every consumer wearable, but they must strictly control how outside device data enters the enterprise network. Establish rigid validation protocols to help ensure unvalidated data from an unmanaged device can't poison central clinical systems.
- **Enforce zero trust across all devices.** Treat every connected monitor and sensor as untrusted until verified. Networks must be architected so that a compromised device is immediately isolated, preventing its data from moving laterally and manipulating broader clinical logic.

WHAT THE DATA SAYS:

HEALTHCARE HAD MORE REPORTED CYBER THREATS THAN ANY OTHER CRITICAL INFRASTRUCTURE SECTOR IN 2024, WITH BOTH RANSOMWARE AND DATA BREACH INCIDENTS INCREASING

Federal Bureau of Investigation Internet Crime Report 2024. April 23, 2025.

#3 Managing ecosystem and vendor risk

Take the still-developing complexities of AI, add the vulnerabilities of connected care, and now multiply that across your suppliers—and your suppliers' suppliers. That is the cyber risk math facing healthcare organizations today. In a highly integrated sector, a breach at a single vendor can quickly become an enterprise-wide crisis.

What leaders need to know

Healthcare ecosystems are inextricably linked, and attackers are aggressively targeting the supply chain. The high-profile ransomware attacks on clearinghouses and medical device manufacturers demonstrate that third-party vulnerabilities can cripple operations both upstream and downstream. When a critical supplier goes dark, the impact cascades: A health system might lose access to vital surgical supplies, for example, or a payer's authorization and payment processes may be frozen. Your organization's resilience depends on the weakest link in your partner network.

The action plan

- **Architect for diversification and failover.** Treat vendor concentration as a critical architectural design flaw. Healthcare leaders must proactively identify single-vendor dependencies that could halt operations and address them with failover redundancies.
- **Shift from compliance to continuous monitoring.** Traditional, paper-based third-party risk assessments are obsolete the moment they are signed. Organizations need continuous supply chain detection and response programs to monitor external threat intelligence and spot vendor vulnerabilities sooner.
- **Enforce shared accountability.** Vendor contracts must explicitly detail cyber security requirements, mandate strict breach communication timelines, and establish automated response plans to quickly isolate compromised third-party connections.

WHAT THE DATA SAYS:

ACROSS SECTORS, ONE-THIRD OF ORGANIZATIONS REPORTED MONETARY LOSS OR REPUTATIONAL DAMAGE FROM THIRD-PARTY RISK EVENTS IN THE PAST THREE YEARS, AND 28 PERCENT FACED SUPPLY CHAIN DISRUPTIONS.

The 2026 KPMG Global Third-Party Risk Management Survey, 2026.

#4 Redesigning security patch cycles—and quickly

Amid the growing sprawl of AI workflows, connected medical devices, and vendor ecosystems, the healthcare attack surface has expanded significantly. Compounding this challenge is the unprecedented speed at which adversaries can now exploit these vulnerabilities. The arrival of advanced, autonomous AI systems threatens to turn the traditional enterprise patch queue into a systemic failure point. By collapsing the time between vulnerability disclosure and exploitation from weeks to hours, AI is rendering human-paced, patch-led security models obsolete.

What leaders need to know

Advanced AI models have fundamentally changed how quickly organizations must respond to threats. Attackers can leverage these models to write the malicious code needed to hack a newly discovered flaw, launching attacks against your network in under 24 hours. Meanwhile, the average time it takes an enterprise to apply a security patch remains at 60 days or more, creating a widening and unsustainable exposure gap. As autonomous systems uncover and share new vulnerabilities at a drastically accelerated rate, relying on traditional patching approaches as your main line of defense is no longer viable.

The action plan

- **Shift from counting patches to managing exposure.** Rather than treating every unpatched system equally, organizations must identify which vulnerabilities are most at-risk and exploitable within their environments. Focus finite patching capacity on critical areas where alternative security measures can't reduce the risk.
- **Automate containment through AI orchestration.** Security teams should centralize data across identity, endpoint, network, cloud, and application layers. By using AI agents to drive detection, organizations can correlate events and trigger automated containment measures across the full attack path.
- **Measure resilience by speed to containment.** Security leaders must target a mean time to respond (MTTR) of under 60 minutes for critical AI-disclosed vulnerabilities. Be prepared to execute pre-authorized, automated actions immediately, rather than waiting for a scheduled downtime window to apply a patch.

WHAT THE DATA SAYS:

ATTACKERS USING AI CAN NOW COLLAPSE THE TIME-TO-EXPLOIT WINDOW TO UNDER 24 HOURS, WHILE AVERAGE ENTERPRISE PATCH CYCLES REMAIN AT 60 DAYS OR MORE.

Claude Mythos: What Frontier AI Vulnerability Discovery Means for Canadian Enterprises

#5 Navigating unrelenting regulatory churn

As cyber vulnerabilities compound across ecosystems, government agencies are aggressively stepping in. Regulators are actively drafting and revising policies to address data privacy, patient safety, and third-party risk, adding a dense layer of compliance complexity to an already strained system.

What leaders need to know

The regulatory environment remains fluid. New mandates are either in motion or under consideration across both federal and state agencies, with potential implications for Centers for Medicare & Medicaid Services reimbursement, updates to the Health Insurance Portability and Accountability Act, and state-level requirements around interoperability and clinical AI usage. The common thread: Regulators want to see demonstrated, continuous operational resilience in the face of inevitable disruptions—and potential liabilities at the executive level are also increasing.

The action plan

- **Shift from compliance to risk management.** Don't treat regulatory updates as isolated, check-the-box projects. Organizations must transition to a comprehensive risk management strategy that positions compliance as a byproduct of strong healthcare security.
- **Prioritize clinical disruption risk.** Healthcare leaders must identify and address the specific vulnerabilities with the greatest potential to halt patient care, applying compensating controls where budgets are tight.
- **Empower clinical teams.** Enhanced security measures cannot come at the expense of patient care. Work directly with clinical leaders to help ensure new regulatory controls are embedded into existing workflows without creating administrative bottlenecks.

WHAT THE DATA SAYS:

7 IN 10 CEOS SAY KEEPING PACE WITH NEW TECHNOLOGY REGULATORY DEMANDS WILL BE A BARRIER TO SUCCESS.

KPMG 2025 Global CEO Outlook.

#6 Preparing for quantum computing threats

Just as leaders grapple with today's digital disruptions, the "exotic" risk of quantum computing is moving off the whiteboard and into reality. This horizon-level threat has the potential to invalidate the encryption algorithms securing decades of historical data. While the technology itself is still maturing, getting ahead of it demands architectural changes today.

What leaders need to know

As part of their broader arsenal, some adversaries are playing the long game with a "harvest now, decrypt later" strategy. Healthcare data has an extended sensitivity horizon—as many as 50 years in some cases. Attackers have already been stealing encrypted genomic records, intellectual property, and clinical trial data. Right now, that stolen data is mostly unreadable ciphertext. But adversaries are stockpiling it, waiting for quantum computing to act as their digital Rosetta Stone—a translation key with the potential to unlock decades of highly sensitive, historical, and now exploitable healthcare data.

The action plan

- **Start the quantum clock now.** Don't wait for quantum computers to hit the market. The transition to post-quantum cryptography will take years, and the planning phase must begin immediately.
- **Conduct a cryptographic asset inventory.** Organizations must know exactly where their sensitive data lives and what specific algorithms currently protect it before they can transition to quantum-safe encryption.
- **Update procurement standards.** Ensure your third-party vendors and new system purchases are capable of supporting quantum-safe standards so you aren't simply building new technical debt.

WHAT THE DATA SAYS:

41% OF ORGANIZATIONS ARE CONCERNED THEY'RE FALLING BEHIND IN PREPARING FOR QUANTUM-DRIVEN SECURITY THREATS AND THE TRANSITION TO POST-QUANTUM CRYPTOGRAPHY.

KPMG Global tech report 2026.

The executive action plan

Most healthcare leaders realize that cyber risk is enterprise risk.

Leading-practice cyber security strengthens current operations, fortifies resilience for the long term, and can deliver a significant competitive advantage. But maintaining that posture requires a daily commitment to security excellence across the organization—and vigilance for what comes next.

Immediate strategies:

- **People:** Build a collaborative risk culture that bridges the gap between the board, security teams, and clinical leadership. Ensure human-in-the-loop oversight is a non-negotiable standard to validate AI-generated clinical insights and preserve patient safety.
- **Process:** Shift from perimeter defense to continuous resilience. Enforce zero trust across all connected medical devices, and extend third-party risk management from static compliance to continuous supply chain detection to prevent vendor-driven outages.
- **Technology:** Establish strict identity governance tailored specifically for non-human identities and AI agents. Concurrently, begin mapping cryptographic dependencies across your systems to prepare for the inevitable transition to post-quantum standards.
- **Regulations:** The era of check-the-box compliance is over. Integrate emerging state and federal mandates into a unified risk management strategy that naturally positions compliance as a byproduct of strong clinical security.

How KPMG can help

At KPMG LLP, we combine deep healthcare industry experience with advanced technical capabilities to help you secure the enterprise without slowing down clinical and operational innovation. We work side by side with payers and providers to navigate these structural shifts and translate cyber security investments into measurable business value.

This approach helps organizations:

- **Strengthen security operations at scale.**
  Our cyber managed services can help healthcare organizations expand monitoring, detection, response, and remediation capabilities while reducing pressure on internal teams. We bring technology-enabled workflows, specialized talent, and scalable delivery models to support more resilient day-to-day operations.
- **Govern AI and non-human identities.**
  We help organizations establish the identity-first frameworks, access controls, human oversight, and monitoring capabilities needed to manage agentic AI, machine identities, and connected technologies with greater confidence.
- **Build ecosystem resilience.**
  We help organizations move third-party risk management from periodic assessments to more continuous, risk-based oversight—helping identify critical dependencies, strengthen vendor governance, and reduce exposure to third-party disruptions.
- **Prepare for regulatory and technology change.**
  Whether organizations are responding to new federal and state requirements, strengthening clinical resilience, or planning for post-quantum cryptography, KPMG helps design security architectures that can adapt as risks, regulations, and technologies evolve.

About the author

Anurag Rai
Global lead, Cyber Security in Healthcare,
KPMG International; Principal, Advisory,
Cyber Security Services
KPMG in the US

Anurag Rai is an Advisory Principal in the KPMG Cyber Security and Technology Risk practice in the United States and serves as the Global Lead for Cyber Security in Healthcare for KPMG International. He works extensively across the KPMG global network to design and deliver integrated cyber security solutions that help healthcare organizations operate securely in an increasingly digital and threat-intensive environment.

Anurag brings more than 20 years of experience across information security, risk management, compliance, privacy, and identity and access management. He has led numerous large-scale cyber security and transformation engagements for major healthcare clients and is widely recognized for his expertise in cyber risk management, trusted AI, and security transformation. He regularly engages with boards and audit committees to provide insights on cyber risk, resilience, and governance.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us in: | **kpmg.com**