



## **Securing the Future of Healthcare:** Cyber Readiness to Reduce Costs, Safeguard Patient Care and Drive Rapid Innovation

## INTRODUCTION

Maintaining robust data and infrastructure security in healthcare is critical to maintain patient safety and operational continuity. The healthcare sector faces an increasingly complex threat landscape—ransomware, data breaches and escalating cyberattacks—compounded by outdated technology and technical debt. To address these challenges, healthcare organizations must prioritize resilience.

Migrating mission-critical systems to the cloud offers a transformative solution, enabling scalability, agility, and innovation while reducing technical debt. However, achieving these benefits requires a strategic approach to advanced security and rapid recovery. This dual focus mitigates risks and enhances patient care, accelerating the path to the real-time health system (RTHS) that leading organizations aim to achieve.

Collaboration with trusted healthcare cybersecurity partners is essential. These partnerships help secure systems, safeguard patient data, and protect critical infrastructure, fostering a resilient culture that prioritizes high-quality patient care and increases patient and provider satisfaction.

## CYBER-RESILIENCE AND SECURITY CHALLENGES

 **Resilience in healthcare is crucial, without it, timely and reliable access to data is compromised, which can critically impact patient care. Any disruption can significantly hinder healthcare delivery, degrading the quality of patient care and, in the worst cases, jeopardizing patient safety.”**  
**David Houlding, Director of Global Healthcare Security and Compliance Strategy**  
Microsoft

According to the [2024 Ponemon Institute’s healthcare report](#), cybersecurity in the industry faces formidable challenges from both external and internal issues. These challenges underscore the importance of transitioning toward an RTHS, where secure, resilient infrastructure enhances uninterrupted access to critical data and optimal patient outcomes.

## EXTERNAL THREATS

Healthcare organizations face significant external threats:

- **Ransomware.** Nearly 92% of healthcare organizations faced a cyberattack last year, averaging \$4.7 million in costs per incident.
- **Third-party risks and supply chain attacks.** These continue to compromise sensitive patient data and disrupt operations.
- **Electronic health record (EHR) vulnerability.** Over a two-year period, healthcare organizations experienced an average of four ransomware incidents, each involving the compromise of EHRs: 36% paid ransoms, with the average payment totaling \$1.1 million.

## INTERNAL CHALLENGES

Internal pressures also undermine cybersecurity:

- **Budget constraints.** Despite a 12% increase in IT budgets, 55% of organizations report a lack of in-house cybersecurity expertise and staffing shortages.
- **Employee negligence.** Human error, including phishing scams and poor compliance with security protocols, accounts for 31% of data loss incidents.
- **System incompatibility.** Mergers and acquisitions exacerbate vulnerabilities. Disjointed security solutions further weaken the overall security posture.

The effect of these cybersecurity threats on patient care is significant. Seventy percent of organizations report ransomware attacks delayed procedures, leading to poorer patient outcomes, increased complications and longer hospital stays. Additionally, 57% of cloud or account compromises disrupted care. These disruptions underscore the urgent need for healthcare organizations to strengthen cybersecurity measures to maintain continuous operations and safeguard patient safety.

Federal agencies **have warned the industry** that EHR systems are prime targets for cybercriminals due to the wealth of sensitive information they store. EHRs contain detailed patient data, including personal identifiers and medical histories, which are highly valuable for identity theft, extortion and fraud on the dark web. EHR systems are a persistent and lucrative target for attackers seeking financial or political gains.

Additionally, research shows that provider mergers and acquisitions in healthcare—**common in the industry**—significantly heighten the risk of EHR security breaches. A recent study found that **data breach risks more than double** the year before and after a merger, mainly due to system incompatibilities and heightened media attention. Integrating disparate EHR systems during these transitions often creates additional vulnerabilities, making it easier for hackers to exploit gaps, which leads to patient data breaches and ransomware attacks.



“Healthcare organizations are under constant cost-reduction pressure, which extends to security teams, security teams are often understaffed, with skilled resources hard to find, costly and difficult to retain. Improving the speed, scale, accuracy and upskilling of these teams is crucial, regardless of security operations center size.”

David Houlding, Director of Global Healthcare Security and Compliance Strategy  
Microsoft



## BENEFITS OF CLOUD-BASED PRODUCTS

The cloud's flexibility and scalability support the swift integration of advanced technologies, strengthening healthcare cybersecurity and enabling clinicians to use cutting-edge tools for patient care. A robust cloud infrastructure aligns directly with the principles of an RTHS, offering the scalability and agility necessary for real-time data processing, rapid innovation and strengthened cybersecurity. With rising cyber threats to EHR systems and health IT infrastructure, healthcare organizations need proven strategies for resilience, including cloud-based security, comprehensive risk mitigation and AI-enhanced security workflows to improve attack readiness.

Healthcare organizations can use the cloud to bolster their cybersecurity posture and reduce technical debt that **plagues the majority of U.S. hospitals**. While complying with federal, state and local regulations is crucial, mitigating cybersecurity risks goes beyond meeting compliance standards.

"Shifting to cloud environments, including hybrid models, requires end-to-end resilience and compliance," Houlding explained. "Healthcare organizations are migrating systems, including EHRs, to the cloud to reduce technical debt, boost agility and focus on advanced applications, including AI. With migrations typically taking months to years, maintaining strong security, resilience and compliance throughout this transition is essential to protect data and ensure seamless access."

AI is transforming healthcare cybersecurity by swiftly identifying and empowering security analysts to address threats across data, systems and applications.

**“AI-driven productivity and cost savings in critical provider systems like the EHR are only possible in the cloud,” “On-premises systems can’t support these advanced functions, limiting innovation in clinical care.”**

**Jaimie Fox, Senior Technology Strategist**  
Microsoft

Balancing innovation with security is crucial as healthcare organizations move to the cloud. Cloud-based security and AI-driven protections allow providers to secure critical systems while advancing clinical innovation.

## EFFECTIVE USE OF AI FOR HEALTHCARE CYBER RESILIENCE


"AI enables security analysts to quickly detect and respond to sophisticated attacks, including phishing, which are growing more prevalent, sophisticated and cheaper to deploy due to attackers' use of AI," said Houlding. "AI also empowers security analysts with real-time context and guidance on response and remediation, greatly enhancing security teams' skills to handle constantly evolving threats."

To enhance EHR recovery, healthcare organizations need a secure, auditable plan that enables rapid, infection-free recovery, protecting patient data from ransomware and enhancing long-term security. Regular security assessments with a zero-trust framework help address vulnerabilities, counter threats and mitigate associated risks. At the same time, integrated, AI-driven solutions improve efficiency, reduce costs and strengthen threat detection and response.

As healthcare modernizes and moves to the cloud, investing in integrated, AI-powered cybersecurity safeguards patient data, builds trust and increases resilience against future risks.

## EHR TO AZURE: A SECURE AND SCALABLE FUTURE

EHRs are critical to healthcare, centralizing patient data to enable accurate, coordinated care and reduce errors. Putting essential systems such as an EHR in the cloud offers healthcare organizations significant scalability, security and innovation advantages, driving innovation and efficiency by supporting data-driven insights, research and advanced technologies like AI and predictive analytics to improve outcomes for individuals and populations.

 **Moving an EHR to the cloud is about building a secure, foundational platform for all connected systems, these interconnected systems, including data from medical devices and other systems, support real-time care, making data accuracy and minimized vulnerabilities essential for patient care integrity."**  
**John Doyle, Global CTO of Healthcare and Life Sciences**  
Microsoft

This integration is a cornerstone of the RTHS model, ensuring that healthcare organizations can provide timely, accurate and secure care while maintaining operational resilience.

"Healthcare is inherently complex and heavily regulated, requiring rigorous standards that many industries don't face," Doyle continued. "Partnering with a platform provider like Microsoft, with expertise in healthcare's unique demands—and with domain-specific partners like Commvault—ensures secure, scalable solutions that meet these standards."

Microsoft's Azure cloud infrastructure provides the flexibility to scale resources as needed, accommodating spikes in demand and reducing technical debt from maintaining on-premises systems.

“In healthcare, integrated security is essential to reducing the inefficiencies and risks associated with multiple, disjointed security tools. Microsoft’s suite, combined with Commvault Cloud’s cyber resilience and recovery capabilities, delivers integrated, AI-powered security. Cloud-based cyber recovery allows for efficient, cost-effective preparedness, enabling healthcare providers to recover quickly from ransomware and other threats while avoiding the costs of on-premises backups.”

John Doyle, Global CTO of Healthcare and Life Sciences  
Microsoft

## MICROSOFT AZURE PLUS COMMVULT CLOUD: CYBER RESILIENCY FOR EHRs ON AZURE

Here’s how Commvault provides cyber resiliency for EHRs on Azure:

- **Comprehensive backup and recovery.** Application-consistent backups safeguard EHR data from cyberattacks, errors and failures, providing data integrity and reliability.
- **Cleanroom recovery for safe testing and recovery.** Isolated recovery environments allow EHR testing, investigation and recovery without affecting production.
- **Immutable air-gap protection.** With a zero-trust framework and unique pre-emptive early warning deception technology, SaaS-based air-gapped storage shields EHR backups from threats.
- **Azure-optimized and cost-effective.** Resilience and recovery instances of both data and the application leverage Azure’s scalability, on-demand cost optimization and unparalleled performance.
- **EHR co-developed integration.** Purpose-built with EHR to provide seamless protection and compliance with regulatory standards.

Microsoft and Commvault deliver streamlined, secure EHR data protection, giving healthcare organizations confidence in data integrity and recovery.

“Commvault is a trusted Microsoft partner, critical for healthcare organizations seeking robust cloud cyber resilience on Azure. As an early participant in the Microsoft Copilot for Security partner program, Commvault uses advanced technology fully integrated with Microsoft security and Azure protection services standards. This makes them an ideal partner for protecting healthcare applications, infrastructure and data in both cloud and hybrid environments.”


Karen Cox, Global Healthcare Partner Strategy Leader  
Microsoft

## BEST PRACTICES FOR OPERATIONALIZING CYBER RESILIENCE

Implementing cyber resilience in healthcare requires a comprehensive approach that includes best practices like conducting regular risk assessments, providing continuing education on cybersecurity policies and procedures, engaging in robust incident response planning and regular testing, and adopting secure recovery processes to protect critical data and infrastructure to maintain seamless operations. Choosing the right strategic technology and services partner can ensure all these tasks are achieved and maintained with required cost-effectiveness.

### 1 Risk assessments: Identify vulnerabilities and focus resources on mitigating high-impact threats.

A comprehensive risk assessment helps healthcare organizations identify and address security vulnerabilities before cyber threats can be exploited.

 **Measuring security posture through risk assessments is vital for identifying gaps and mitigating risks. Risk assessments and trusted compliance frameworks also help direct limited resources to where they can best improve security and lower risk.”**  
**David Houlding, Director of Global Healthcare Security and Compliance Strategy**  
Microsoft

During a risk assessment, security teams identify and prioritize data confidentiality, integrity and availability threats. While it cannot prevent cyberattacks, a risk assessment focuses limited resources on top-priority risks in terms of likelihood of occurrence and impact, strengthening data protection and enhancing visibility with monitoring, detection and early warning, response and recovery—making it more difficult for attackers to succeed, and significantly reducing the impact of cybersecurity incidents.

Microsoft’s recently released [2024 Healthcare Threat Intelligence Ransomware Report](#) highlights the latest findings on the impact of cyberattacks and the “ransomware ripple effect” that hinders not only the attacked institution but also nearby institutions, all of which can help you build a case for increased focus on and investment in your cyber-readiness plan.

### 2 Robust cybersecurity policies and procedures: Strengthen network segmentation, enforce multifactor authentication (MFA) and secure medical devices.

After identifying security gaps through risk assessments, healthcare organizations should strengthen cybersecurity controls and tighten procedures to minimize cyberattack risks. Segmenting critical systems within the network, for example, is an effective safeguard to help prevent lateral movement by threat actors, reducing the impact of cybersecurity incidents such as ransomware and disruptions to patient care.

Security practitioners should proactively address known vulnerabilities and secure exploitable medical devices. The Cybersecurity and Infrastructure Security Agency warns that common weaknesses in healthcare include web application vulnerabilities and unsupported software configurations.



Ensuring that all systems are protected by MFA is another way to reduce the occurrence and impact of cyberattacks. [Data from the HHS 405\(d\) Program](#) showed that while over 90% of hospitals use MFA, its inconsistent application creates gaps. Implementing MFA across all systems strengthens network security and hinders threat actors.

Data backups and strong encryption are also critical for saving time and money during a breach. Proven best practices, including network segmentation, MFA, least privilege across roles and over time and vulnerability management can help organizations mitigate risks and prepare for attacks.

The just-released [2024 GigaOm Healthcare Cyber Recovery Readiness Report](#), developed in partnership with Commvault, provides a blueprint for organizations to improve their readiness and resilience before the next attack hits.

### **3 Incident response planning and practice: Conduct regular periodic testing to prepare for cyber events.**

The first step is acknowledging that a cyberattack or data breach will likely occur. From there, security experts can plan protection, monitoring, detection, response and recovery efforts in preparation for an incident. Incident response plans—along with data backup, cyber recovery and emergency mode operation plans to maintain compliance—should include communication strategies, alternative ways to access patient records during EHR system downtime and procedures to enhance the availability of critical healthcare data. After containing a threat, the focus shifts to executing a recovery plan that restores data and systems as quickly as possible.

Healthcare organizations must be prepared to engage with stakeholders, legal counsel, PR, law enforcement and patients when a cyber incident occurs. Testing and preparing with key stakeholders before a cyberincident can ensure plans are accurate, complete and up to date and help organizations respond more efficiently and effectively amid an actual cyber event. Commvault's critically acclaimed [Minutes to Meltdown](#) immersive events actually take participants through the reality of an attack,



engaging executives and IT practitioners in the experience of an attack and sharing the expertise and guidance of some of the most renowned cybersecurity experts across the globe; a healthcare-specific version is available.

**“Cloud providers offer superior security compared to individual hospitals, enabling healthcare organizations to implement more effective response and recovery plans while securely shifting infrastructure and focusing on innovation and efficiency.”**  
**Jaimie Fox, Senior Technology Strategist**  
Microsoft

While a cyberattack may be inevitable, conducting risk assessments, employing security best practices and practicing incident response and recovery are domains that healthcare organizations can control.

## REAL RESULTS DRIVE PREPAREDNESS AND ENSURE CONTINUOUS PATIENT CARE

“In my dual roles, I see both perspectives,” said Umang Patel, NHS pediatrician and chief clinical information officer at Microsoft. “At Microsoft, I understand the importance of incident recovery, but as doctors, we simply expect reliable, secure technology. If systems fail or are breached, patient care suffers—we can’t conduct clinics, order tests or review X-rays essential for diagnosis. Reliable systems are crucial for delivering effective healthcare at scale.”



At the British Medical Association (BMA), CISO Peter Hands has worked on enhancing the organization’s incident response capabilities and overall cyber-resilience, particularly improving visibility across systems and developing cloud “landing zones.” These cloud templates incorporate best practices in security, compliance, observability and resilience. By refining incident categorization and clearly defining roles and responsibilities, he aims to enable faster and more effective responses to cyber incidents.

**“Protecting infrastructure and data backups is crucial because, without data, we cannot operate or fulfill our mission. Beyond operational risks, data loss threatens our reputation, incurs regulatory fines and leads to other costs. Ultimately, our goal is to keep the organization running smoothly so we can better serve patients nationwide.”**  
**Peter Hands, Chief Information Security Officer**  
British Medical Association (BMA)

Effective cybersecurity incident response goes beyond reactive measures, instead relying on thorough preparation, clearly defined roles, and consistent practice. Partnering with Microsoft and Commvault, BMA has integrated advanced technologies to safeguard healthcare data, enable data integrity during recovery and maintain continuous operations.

**“Cyber recovery isn’t like a typical outage—you need to be sure your data is safe and uncompromised before restoring it, or you risk making things worse. Microsoft and Commvault seamlessly share threat signals, enabling security and IT teams to work within their usual tools without switching apps. Commvault Cleanroom Recovery allows teams to practice secure data recovery, ensuring readiness for real incidents. Microsoft Copilot for Security further accelerates response, helping analysts work faster and sharpen their skills. These tools prepare teams to handle cyberincidents with confidence and precision.”**

**Peter Hands, Chief Information Security Officer**  
British Medical Association (BMA)

## CONCLUSION

Securing the future of healthcare requires a commitment to resilience, innovation and cost efficiency. By embracing cloud-based infrastructure, healthcare organizations can strengthen cybersecurity, compliance and their ability to monitor, detect and respond to cyberthreats, protecting critical data and supporting the continuity of patient care.

Collaborating with trusted partners who understand healthcare’s unique demands enables organizations to build secure, scalable systems that reduce technical debt, enhance compliance and foster rapid innovation while accelerating the path to an RTHS reality. In doing so, healthcare leaders safeguard data and reinforce the foundation for reliable, high-quality patient care in a rapidly evolving IT and threat landscape.

### Contributors:

**John Doyle**, Global CTO of Healthcare and Life Sciences, Microsoft

**David Houlding**, Director of Global Healthcare Security and Compliance Strategy, Microsoft

**Karen Cox**, Global Healthcare Partner Strategy Leader, Microsoft

**Jaimie Fox**, Senior Technology Strategist, Microsoft

To learn more, visit [commvault.com](https://commvault.com)



commvault.com | 888.746.3849

© 2025 Commvault.

