How MSPs can build practices in the high-growth health care sector

The stakes for cybersecurity in health care are extremely high. System failures and downtime can have catastrophic effects on patients. Unfortunately, many health care organizations struggle to manage cybersecurity effectively. Managed service providers (MSPs) have a significant opportunity to step in and help, while also driving revenue.

Data from the 2025 Black Book Market Research report illustrates the scope of the challenge:

68%

of health care providers say they can't address cyber risks adequately because of insufficient funds.

60%

Nearly 60% of health care organizations report challenges in hiring and retaining skilled IT professionals.

28%

of breaches are accounted for by human error, with threats from inside the organization primarily due to phishing.

As a result, adoption of managed security services in health care grew by 35% from 2024 to 2025. The opportunity for MSPs is large and growing.[1]

A need to go beyond standard managed services

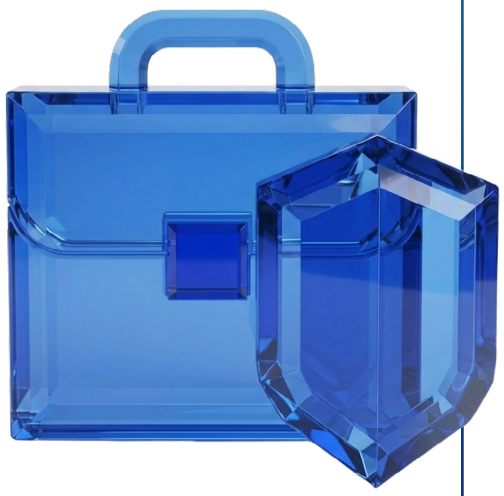
Clinical environments rely on always-on systems such as electronic health records, imaging platforms and patient monitoring tools. A failure in any of those systems impacts patients directly. MSPs can move beyond traditional IT support and become essential partners in keeping critical systems up and running, and ensuring clinical continuity, security and compliance.

However, succeeding in health care requires more than standard managed services. MSPs need to be able to manage complex regulatory requirements, secure legacy medical systems and deliver near-zero downtime in environments where every minute is precious.

[1] Black Book Market Research, The Black Book of Healthcare Cybersecurity: 2025 Edition

Business and technological challenges

Succeeding in the health care sector isn't easy. Serving health care clients offers a series of challenges many service providers might not be familiar with. MSPs face a unique combination of operational pressure, security risks and technical complexity.



The impact of downtime on patient safety

Health care organizations cannot tolerate outages. System failures can delay treatments, divert patients and disrupt critical care workflows. Plus, downtime is expensive. The average cost of a data breach for health care organizations is $7.42 million, according to IBM.[2] MSPs must deliver near-zero recovery time objectives and consistently high availability.

Expanding attack surface from legacy systems

Health care environments continue to depend on legacy infrastructure and connected medical devices. Many of those systems cannot be patched without disrupting care, so MSPs end up being responsible for securing outdated and vulnerable technologies.

The high value of health care data to cybercriminals

Protected health information is among the most valuable data on the dark web and in the criminal underground. As a result, health care organizations are prime targets for ransomware and data theft. MSPs must deliver advanced protection and rapid recovery.

Rising ransomware threats

Ransomware attacks targeting health care continue to grow. The FBI says that reported ransomware incidents targeting health care organizations rose 93% from 2024[3] to 2025.[4] Attackers exploit the urgency of clinical operations. MSPs must implement layered defenses that include prevention, detection and reliable recovery.

Complex hybrid environments

Health care IT environments span on-premises systems, cloud platforms and specialized clinical applications. Maintaining secure interoperability across systems such as electronic health records (EHRs) and imaging platforms adds significant technical complexity.

Tool sprawl and operational inefficiency

Many MSPs rely on multiple disconnected tools for backup, security and management. That approach increases operational overhead, creates visibility gaps and reduces response efficiency during incidents.

[2] IBM. (2025). Cost of a data breach report 2025: The AI oversight gap. IBM & Ponemon Institute.

[3] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2024). 2024 Internet Crime Report.

[4] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2025). 2025 Internet Crime Report.

Industry and operational challenges

Beyond technical hurdles, working with clients in health care involves strict regulatory and operational demands.

Regulatory compliance and audit pressure

MSPs must meet strict compliance requirements, often assuming legal liability. Audit readiness and documentation are critical but can be resource intensive.

Data integrity and trust concerns

Health care organizations must ensure the accuracy and integrity of clinical data. Silent data corruption and inconsistent records can lead to serious diagnostic risks MSPs must mitigate.

Imaging and data performance requirements

Medical imaging systems generate massive datasets that must always be available for instant access. MSPs need to design hybrid architectures that balance performance with secure storage.

Cost constraints

Health care organizations often operate with limited IT budgets despite growing security demands. MSPs must deliver high levels of protection while maintaining cost efficiency.

A platform built for health care MSPs

To succeed in health care, MSPs need a platform that delivers security, data protection and operational efficiency in a single solution. Acronis Cyber Platform enables MSPs to protect the entire clinical environment while simplifying operations and improving profitability.

With Acronis Cyber Platform, MSPs can:

Guarantee clinical continuity

- Ensure critical systems remain available with instant restore and near-zero recovery times.
- Maintain access to EHRs, imaging systems and bedside devices even during cyber incidents.

Secure the entire health care environment

- Protect modern cloud platforms and legacy medical systems with a single integrated agent.
- Reduce risk across endpoints, workloads and internet of medical things (IoMT) devices.

Simplify compliance and audit readiness

- Automate compliance processes with data protection maps and audit-ready reporting.
- Transition from basic IT services to high-value compliance offerings.

Restore with confidence

- Enable malware-free recovery with safe recovery capabilities.
- Scan and clean backup data before restoration.

Reduce complexity and improve margins

- Eliminate tool sprawl by consolidating backup, security and management into one platform.
- Improve technician efficiency and increase service profitability.

Acronis Cyber Platform: Capabilities designed for the health care industry

Acronis delivers a comprehensive set of capabilities designed specifically for health care environments:

Unified cyber protection platform: Acronis combines cybersecurity, backup, disaster recovery and endpoint management in a single platform, reducing operational complexity and improving visibility.

Advanced backup and recovery: MSPs can protect critical systems with image-based backup, immutable storage and fast recovery for clinical and imaging environments.

Endpoint protection and EDR: With endpoint detection and response (EDR), service providers can secure clinical workstations, servers and remote endpoints.

Automated compliance and data protection: Acronis Cyber Platform enables MSPs to identify and protect sensitive health data with automated discovery tools and centralized reporting for audit readiness.

Microsoft 365 protection: With many health care organizations using the popular productivity suite, MSPs can ensure continuity for Microsoft 365 and other communication and collaboration tools, including email, file storage and patient coordination platforms.

Support for legacy systems: MSPs can extend protection to older operating systems and specialized medical equipment without requiring disruptive upgrades.

Forensic backup and data integrity: Service providers can capture forensic data for incident investigation and ensure record integrity with blockchain-based verification technologies.

The Acronis Cyber Platform advantage

Unlike point solutions loosely cobbled together, Acronis delivers a natively integrated platform with a single point of management that enables MSPs to:

- Deliver complete cyber protection across health care environments.
- Reduce operational overhead and tool sprawl.
- Improve response times and recovery outcomes.
- Expand into high-value compliance and security services.
- Increase margins while scaling health care offerings.

With essential capabilities consolidated into a single platform, MSPs can cut costs and simplify operations while delivering the resilience health care organizations demand.

Start growing your health care practice

Health care organizations need trusted partners to ensure continuity, security and compliance. Acronis Cyber Platform enables MSPs to capture the opportunity with confidence.

↘ Book a demo to see how Acronis supports MSPs working with health care clients

↘ Start a trial and begin delivering resilient MSP health care services today

Acronis

Learn more at acronis.com