UNDER PRESSURE:

The 2026 Healthcare IT Landscape Report

Exploring How the Confluence of Vendor Risk, Compliance Mandates and AI Adoption Strains Today's Healthcare Leadership

omega systems
technology managed

UNDER PRESSURE:
Healthcare IT Landscape Report
2026

omega systems
technology managed

Table of Contents

62%

of healthcare leaders still treat cybersecurity as a technical expense rather than a clinical or fiduciary risk.

Report curated by
omega systems

Executive Summary

The biggest cybersecurity threat facing healthcare practices in 2026 is not a sophisticated hacker. It is the vendors those practices already trust – and have stopped questioning.

This finding anchors Omega Systems' 2026 Healthcare IT Landscape Report, which surveyed 200 C-suite executives, IT leaders, and practice administrators across independent and mid-market healthcare organizations. The results reveal a sector navigating compounding pressure: a widening third-party attack surface, an accelerating fatal-incident trajectory, a compliance environment that has run out of flexibility, and an AI opportunity that most practices cannot yet safely capture.

Running beneath all of it is a single root cause. Sixty-two percent (**62%**) of healthcare leaders still treat cybersecurity as a technical expense rather than a clinical or fiduciary risk. That posture determines what gets funded, what gets deferred, and what gets ignored. It is why the gaps documented in this report persist despite years of escalating threat data.

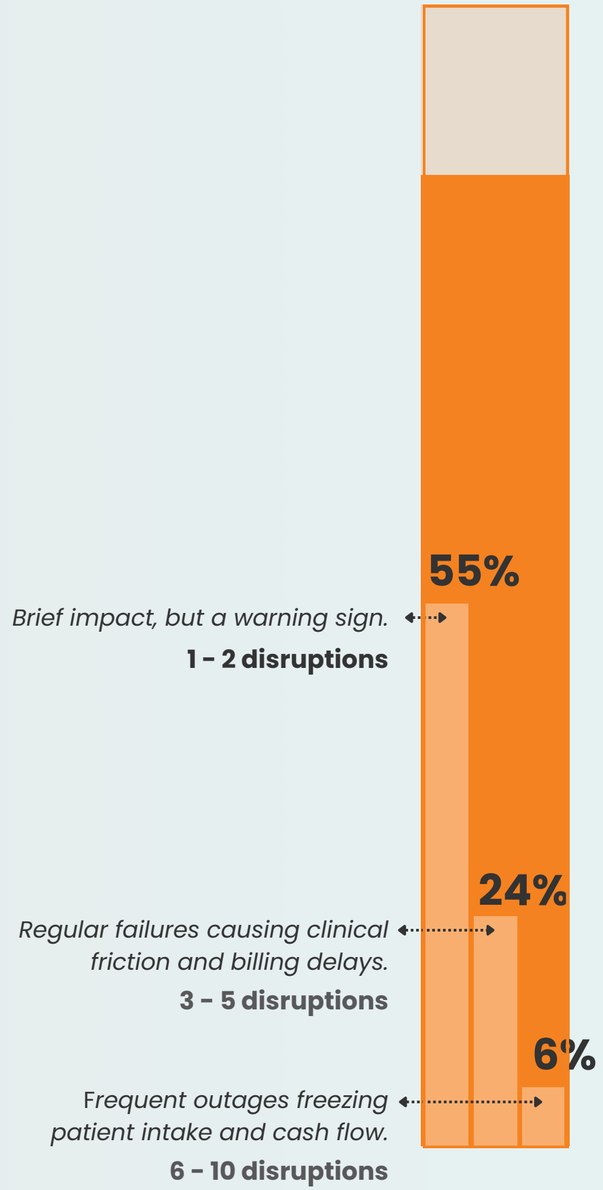
The practices that will lead in the year ahead are not the ones with the most advanced technology. They are the ones that have made a governance-level commitment to treating security, compliance, vendor risk, and AI not as separate problems requiring separate solutions, but as one – with a partner accountable for the whole picture.

The Biggest Cyber Threat to Healthcare Isn't Hackers. It's Vendors You Trust.

Think about what it takes to run a modern healthcare practice. There's an EMR system for clinical records, a billing platform for claims and collections, a telehealth tool for remote visits, a cloud storage provider for data, and a patchwork of other vendors keeping operations running behind the scenes.

Each connection is essential. Each connection is also a door that someone else controls. That's not a hypothetical risk. Eighty-five percent (**85%**) of practices experienced at least one operational disruption caused by a third-party or "vendor-of-a-vendor"* failure in the past 12 months.

* ***What Is a "Vendor-of-a-Vendor" Breach?***
A vendor-of-a-vendor breach happens when a company your vendor relies on gets attacked — and the damage flows downstream before you even know there's a problem. Your practice never interacted with the original target. But when an EMR vendor's cloud storage provider gets compromised, or a billing platform runs on software from a hacked developer, patient data and operations are affected anyway.



85%

of practices experienced at least one operational disruption caused by a third party in the last 12 months

What makes this particularly alarming is not the frequency. It's the confidence gap that sits alongside it.

Seventy percent (**70%**) of leaders say they are "confident" or "very confident" in their vendors' cybersecurity posture – even as **24%** of respondents report experiencing a third-party or vendor breach that directly affected their data or operations in the past year. More revealing: **24%** simultaneously name “not knowing their vendor network's security posture” as one of their top IT anxieties. Confidence and visibility are not the same thing, and attackers understand that better than most healthcare practices.

Consider this: 63% of practices do not continuously monitor their networks and digital supply chains – yet **70%** say they’re confident in the vendors connected to them.

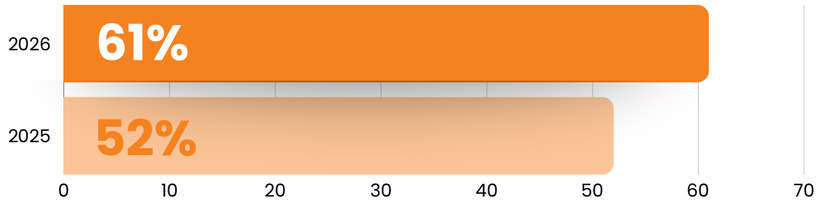
A practice can’t be confident in what they aren’t watching.

Trust is a natural byproduct of long-term vendor relationships. And that’s precisely what attackers count on. They target vendors because their healthcare clients trust them – and rarely verify the controls behind that trust.

The third-party attack surface is wide, growing, and under-monitored. For healthcare practices that have not yet experienced a consequential breach through a vendor connection, that may reflect good fortune more than a strong defense.

Most Healthcare Leaders Believe a Cyberattack Will Kill a Patient Within Five Years.

Sixty-one percent (**61%**) of healthcare leaders say a fatal patient incident caused by a cyberattack at a U.S. healthcare facility is inevitable within the next five years – up from **52%** in 2025, a relative **17%** increase in just 12 months.



Belief and preparedness are moving in opposite directions.
While the share of leaders who see a fatal incident as inevitable has grown nearly 10 points in a year, the systems, staffing, and recovery plans needed to prevent it have not kept pace. The gap between what leaders expect and what their practices are ready for is where the real risk lives.

The belief is widespread. The preparedness is not. Consider what happens at the moment a practice's EMR goes down due to a cyberattack.

- **53%** say billing, claims, and scheduling would stop instantly – freezing cash flow at the exact moment clinical operations are most compromised.
- **47%** say loss of access to patient histories and medication lists would create immediate safety and malpractice liabilities.
- **25%** say the inability to maintain baseline care standards would force temporary or permanent closure.

These are not edge-case scenarios. **They are the predictable consequences** of the security posture most practices currently maintain. And the data shows the gaps are significant.

Alarming statistics reveal critical gaps in cyber resilience and recovery preparedness

Rely on on-premise infrastructures and/or legacy cloud systems that lack the capabilities to contain and resolve data breaches quickly

Do not train their teams on incident response regularly

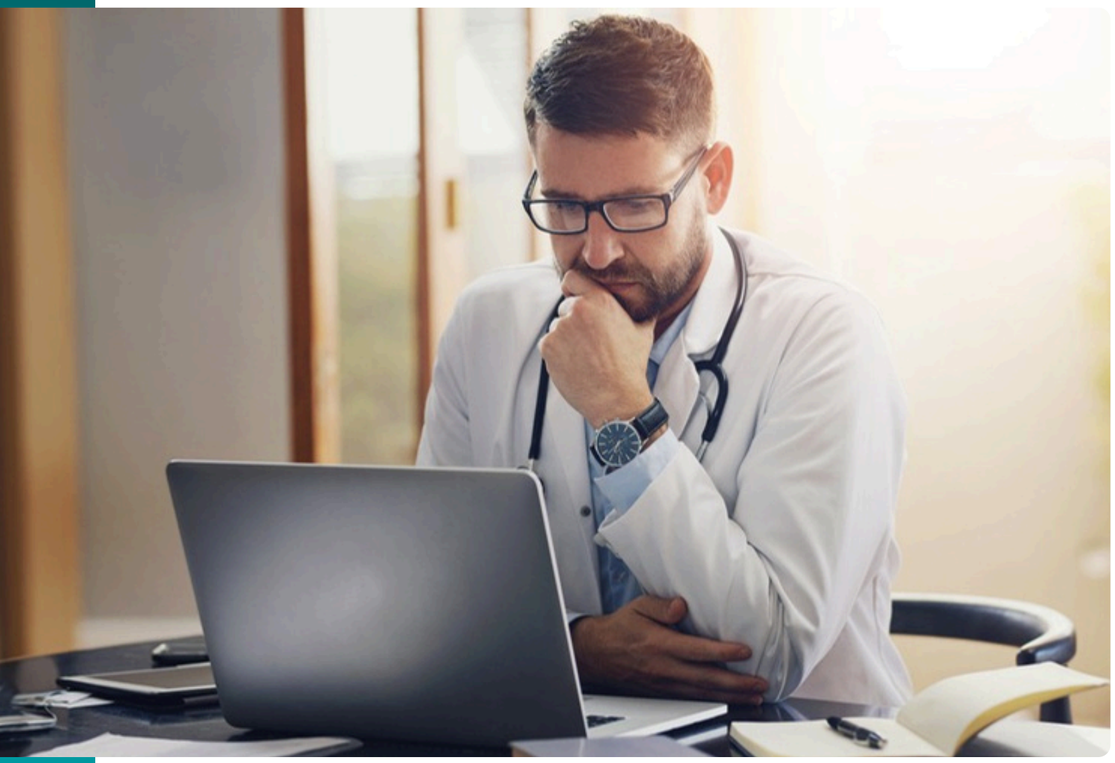
Have no independent recovery path and would have to wait indefinitely for their EMR system or cloud provider to come back online

Do not have access to a 24x7 SOC team (in-house or outsourced)

Have no documented recovery plan at all

Only 18% of healthcare providers feel fully prepared to **recover from a cyberattack.**

82% of healthcare providers acknowledge meaningful gaps in their recovery readiness.



In fact, when asked what factors would hinder their ability to recover from a significant cyber incident, only 18% of respondents said "none of the above." That means more than eight in ten practices **(82%)** acknowledge meaningful gaps in their recovery readiness.

The stakes could not be clearer. The sector has already seen cyberattacks delay surgeries, divert emergency patients, and compromise medication administration. The leaders surveyed know what's coming. The question is why more practices have not yet taken the steps necessary to reduce the likelihood they become the example others learn from.

Most Common Cyber Threats in Healthcare *(experienced in last 12 months)*

28%
Phishing or Smishing Campaign

24%
Third-party or Vendor Breach

17%
Business Email Compromise

16%
Insider Threat or Data Compromise

14%
Cloud Infrastructure Attack

Healthcare's Cybersecurity Gap Starts at the Top.

The vendor risk is real. The preparedness gaps are real. But the data reveals something more fundamental than a technology gap – it reveals a leadership one.

Sixty-two percent (**62%**) of leaders agree with this statement:

> ***"Our organizational leadership views cybersecurity as a technical expense rather than a clinical or fiduciary risk."***

That's not a technology problem. That's a governance problem, and it shapes every investment, staffing, and prioritization decision that follows.

When security is a cost center, the consequences reach further than the budget line:

35% of healthcare organizations say their cyber and IT team is understaffed.

26% say their cyber and IT team is underfunded.

33% underestimate the severity and frequency of the attacks they're facing.

21% acknowledge they deliberately downplay cyberattack risk to avoid reputational damage.

With this insight, the resulting technology gaps are predictable. Despite the known threat landscape:

52% have no MSSP partner – and 11% have no plans to engage one.

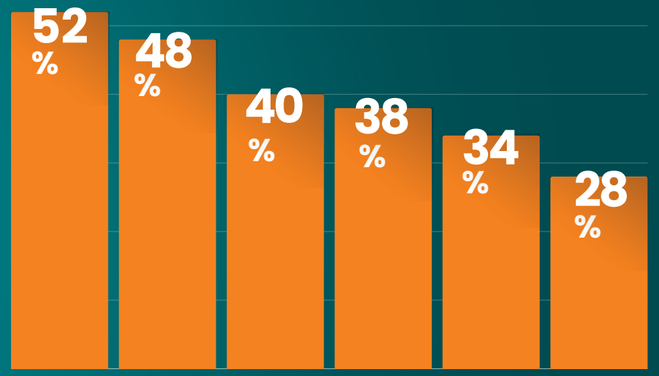
48% are still running legacy systems and applications.

40% do not proactively conduct vulnerability or IT risk assessments.

38% are not offering cybersecurity awareness training to staff.

34% do not require multi-factor authentication.

28% still have no password management system in place



Consider this: The top cybersecurity challenge healthcare leaders report today **(26%)** is not a shortage of solutions – it's staying current on evolving requirements. The tools exist. Expertise exists. What's missing, in too many practices, is the organizational will to prioritize the investment.

It's worth noting that this is not the full picture. Forty-one percent (**41%**) of practices plan to partner with an MSSP in the next 12 months – a meaningful signal that the sector is beginning to shift. But the practices moving in that direction are not waiting for a breach to motivate them. They are making the governance decision that security is a business priority, not a line item to be deferred.

The gap between knowing the risk and funding the response is where most practices remain stuck. Vendor threats, recovery failures, and projections of fatal incidents are the consequences that live in that gap.

41% of practices plan to partner with a managed security provider (MSSP) in the next 12 months.

Most Practices Are Signing Off on HIPAA Compliance They Know Is Incomplete.

When leadership treats cybersecurity as a technical expense, compliance tends to follow the same logic. It becomes a box to check rather than a standard to meet. The data shows exactly what that looks like.

Six in ten healthcare leaders admit they have self-attested to HIPAA compliance while knowing their own risk assessments flagged unresolved vulnerabilities.

That means almost **two-thirds** of practices are operating with a compliance posture they know to be incomplete. But it's worth understanding why before rushing to judgment. For most healthcare organizations, the gap between knowing and fixing isn't negligence – it's math. Budget is limited, internal expertise is stretched, and the previous HIPAA framework offered enough interpretive flexibility that deferring remediation felt manageable. Practices made a calculated trade-off: keep the doors open, keep patients served, and address the gaps when resources allow.

Do this regularly
signing off while routinely deferring remediation.

Do this occasionally
leaving technical gaps open while focusing on patient care

Never attest
until all identified risks are fully remediated

23%

of practices **have already filed a breach notification with the HHS Office for Civil Rights.** For many, that filing was not the result of negligence. It was the result of a gap that grew faster than their resources could close it. Small practice leaders are not ignoring compliance. They are managing it with teams that are stretched thin, budgets that do not go far enough, and requirements that keep changing. The breach notification is often the moment they find out how serious that gap had become.

The proposed 2026 HIPAA Security Rule closes that window. For the first time, the requirements are specific, time-bound, and binary: either practices have written 72-hour recovery procedures, or they don't. Either they've run a vulnerability scan in the last six months, or they haven't. Either their business associates have been verified this year, or they haven't.

There is no longer a defensible middle ground, which makes the finding that only **24%** of practices are fully prepared for these changes not just a compliance gap, but an urgent operational one.

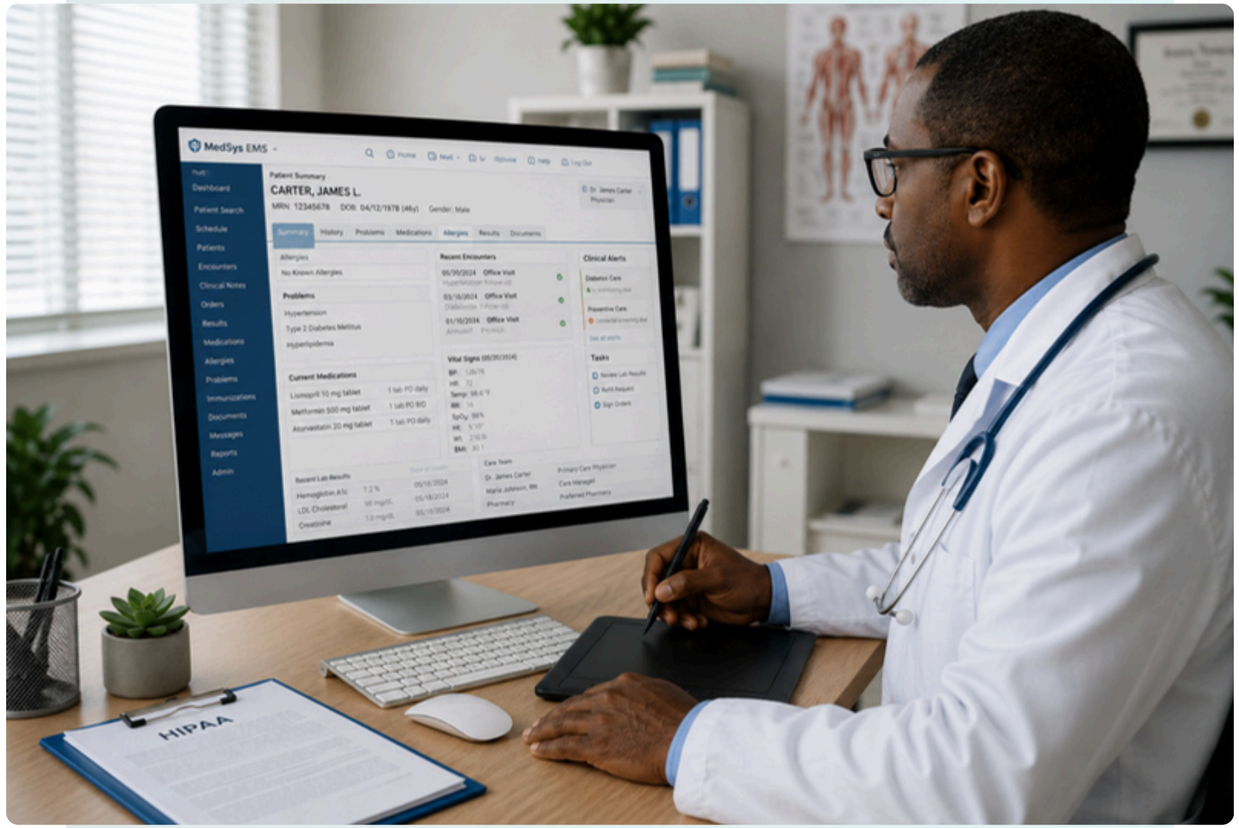
The areas of unreadiness reflect exactly the kind of controls that have historically been deferred:

- **28%** cannot yet meet the requirement to develop written procedures for restoring data within 72 hours, including restoration priority based on system criticality.
- **26%** cannot yet meet the requirement to conduct vulnerability scans every six months and an annual penetration test.
- **25%** have not yet implemented multi-factor authentication (MFA) across all staff.
- **25%** cannot yet meet the annual verification requirement for business associates' and contractors' security measures.

These are not new concepts. MFA, vulnerability scanning, and recovery planning have been recognized as best practices for years. What the 2026 HIPAA proposal does is remove the flexibility that allowed practices to acknowledge those gaps without being required to close them on a fixed timeline. **For practices that have been deferring, the clock is no longer hypothetical.**

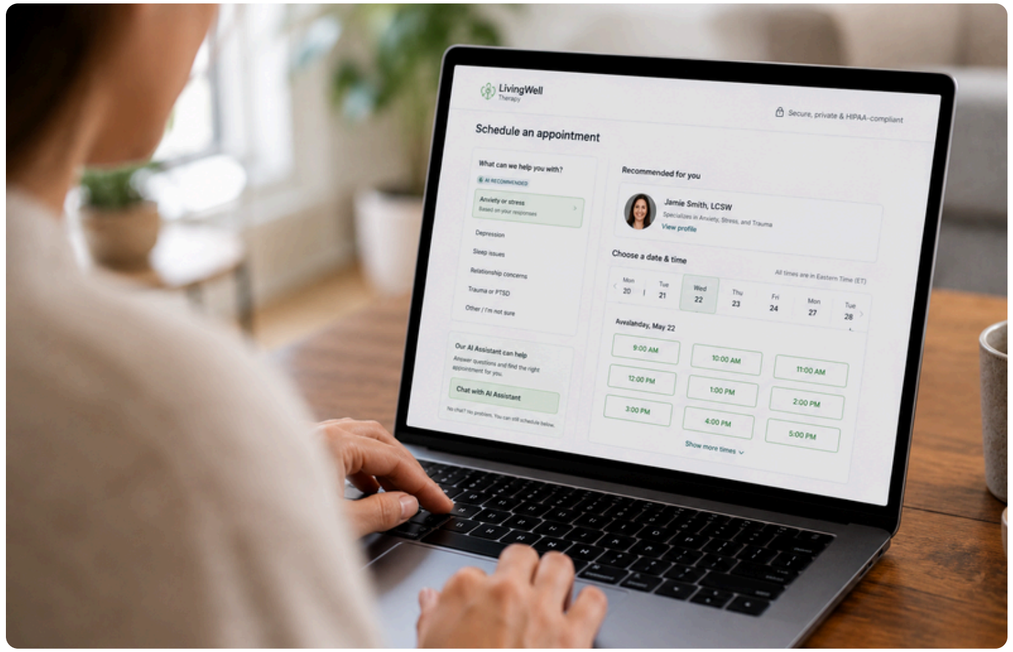
The structural barriers to getting there are significant. Lack of internal expertise on changing HIPAA compliance standards and limited budget for data privacy and compliance remain the most consequential obstacles. Practices understand what's required, but understanding a requirement and having the capacity to meet it are two very different things.

The expected 2026 mandates have effectively ended the era of reactive compliance. Waiting for the annual assessment cycle, patching the most visible gaps, and signing off on the rest is no longer a viable strategy. Requirements are specific, and the enforcement timelines are firm. The practices that will meet these requirements aren't doing more paperwork – they're operating under a continuous compliance program, with monitoring, automated evidence collection, and expert guidance built-in from the start.



AI Is Already Here. Most Practices Can't Fully Harness It.

The compliance pressure healthcare organizations are facing today doesn't exist in isolation. It lands on practices that are simultaneously navigating a technology landscape that is moving faster than their resources allow. Nowhere is that tension more visible – or more consequential – than in how medical practices are approaching artificial intelligence (AI).



The conversation around AI in healthcare has shifted. It is no longer a question of whether independent practices will adopt it – **93% already have**. The question now is whether the infrastructure, expertise, and organizational appetite exist to capture what it's actually worth.

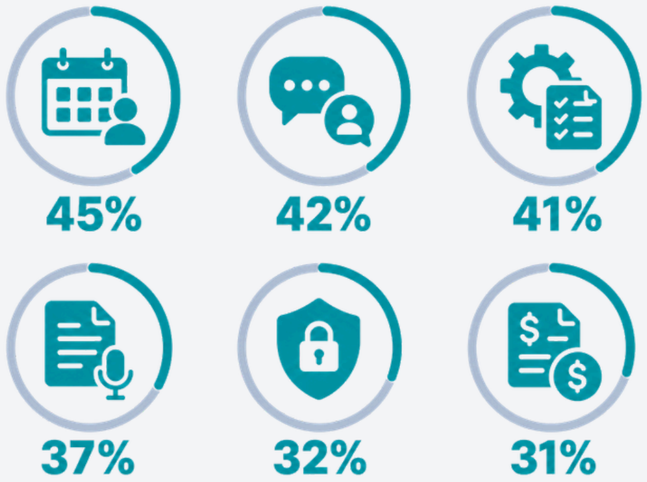
The revenue case for AI is more concrete than most leaders realize. When asked to estimate the impact of allowing staff to see just two additional patients per day through AI-enabled scheduling, practice leaders were clear:

Estimate $5,001 - $10,000
in additional monthly gross revenue (MGR)

Estimate $10,001 - $20,000
in additional monthly gross revenue (MGR)

Estimate $20,001 +
in additional monthly gross revenue (MGR)

That puts the recoverable revenue opportunity from a single, modest AI use case somewhere **between $5,000 and $20,000 per month** for roughly two-thirds of practices surveyed – before accounting for gains in billing accuracy, prior authorization speed, or clinical documentation time. This is not a speculative ROI projection. It is what practice leaders themselves estimate, based on their own patient volume and revenue per visit.



The adoption data reflects how seriously practices are already treating that opportunity. AI is being deployed across a wide range of functions:

AI Adoption Among Medical Practices

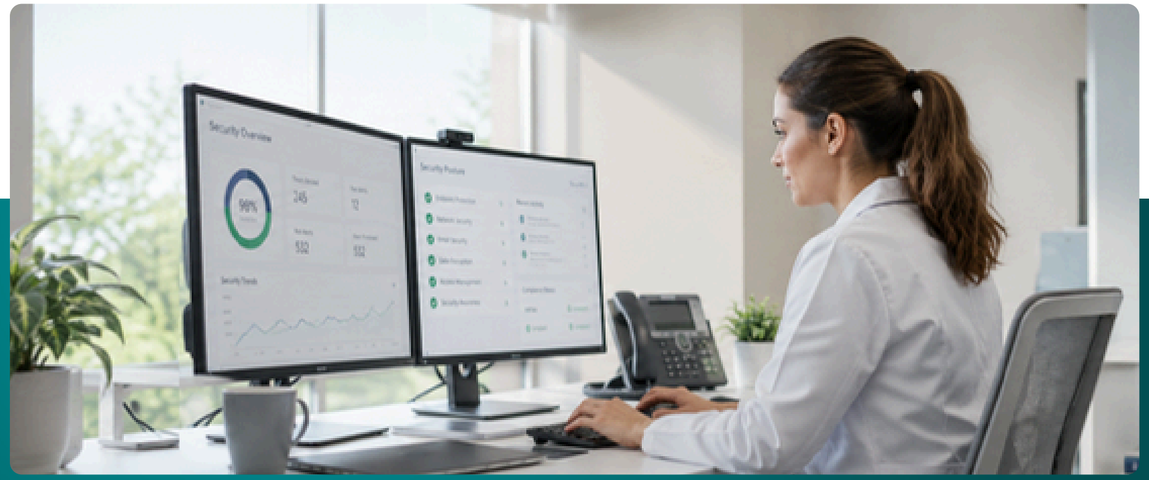
Scheduling, intake, and front desk operations	**45%**
Patient engagement and communication, including chatbots, messaging, and reminders	**42%**
Administrative workflow automation, such as prior authorization and internal processes	**41%**
Clinical documentation, including scribing and note generation	**37%**
Cybersecurity threat detection and monitoring	**33%**
Revenue cycle management, including billing, coding, and claims processing	**31%**

Despite near-universal adoption of AI, **28%** of practices still feel behind – and the barriers they cite reveal why the revenue opportunity remains out of reach for so many:

- **26%** say the cost of AI tools is too significant for their small IT/security budget
- **23%** say AI tools today lack a proven, clinical-grade ROI or a clear path to seeing more patients per day
- **22%** cannot verify that emerging AI tools meet the new HIPAA mandates
- **21%** say leadership views AI as a back-office expense rather than a revenue-recovery engine, resulting in a total lack of investment

The infrastructure gap behind these barriers is worth naming plainly. AI tools that touch patient scheduling, clinical documentation, or billing data operate within the same HIPAA framework as every other practice system. **Every new AI vendor is a new connection** into that environment.

Deploying them without verified HIPAA alignment or secure data integration doesn't just create compliance exposure. It creates the kind of third-party risk highlighted earlier in this report. The practices positioned to capture AI's revenue upside are not the ones with the most tools. They are the ones who have built the foundation that makes deploying those tools safely possible.



The In-House Security Model is Broken.

The right foundation makes everything else possible. The data from this report illustrates that most healthcare practices do not yet have it. And the model most are relying on to build it was never designed for the environment they're operating in today.

That is not an indictment of the people managing security inside these organizations. It is an indictment of the model itself. In-house cybersecurity and compliance programs were built for a simpler threat landscape, a less demanding regulatory environment, and an attack surface that didn't include dozens of third-party vendor connections, AI tools handling patient data, and remote care workflows extending the perimeter in every direction. The threats have evolved. The model, for most practices, has not.

The numbers reflect that gap plainly. Today:

- **35%** say their cyber/IT team is understaffed
- **33%** underestimate the severity and frequency of cyberattacks
- **26%** report their cyber/IT team is underfunded
- **24%** don't know the cyber risks across their own perimeter
- **23%** say their cybersecurity technology is antiquated
- **21%** are deliberately downplaying cyberattack risk to avoid reputational damage

These are not isolated weaknesses. They are the predictable outputs of a model that asks internal teams to do more than their staffing, budget, and expertise can sustain. And they show up directly in the technology decisions practices are making – or failing to make:

- **52%** have no MSSP partner – and 11% have no plans to get one.
- **48%** are still running legacy systems and applications.
- **40%** don't proactively conduct vulnerability and IT risk assessments.
- **38%** are not offering cyber awareness training to staff.
- **34%** do not require multi-factor authentication (MFA).
- **28%** still have no password management system in place.

Taken individually, each of these gaps is addressable. Taken together, they describe an organization that is managing cybersecurity reactively, without the visibility, staffing, or infrastructure to get ahead of the threats this report has documented from its first page.

The shift away from this model is already underway – and the data suggests it is accelerating. Forty-one percent (**41%**) of practices plan to partner with an MSSP in the next 12 months.

Those with existing partners are adopting more advanced technologies to keep up with the changing landscape:

- **43%** are adopting endpoint protection (EDR) with automated moving target defense technology.
- **42%** are implementing managed threat detection & response (MDR).
- **35%** are implementing next-gen firewalls and perimeter security.
- **31%** are implementing data discovery and classification technology.

The practices closing their security gaps are not the ones investing more in their in-house teams. They are the ones who have made a different organizational decision – that security, compliance, vendor risk, and AI governance are not functions to be managed on the margins of an already stretched team, but outcomes to be held accountable by a partner with the expertise and infrastructure to deliver them continuously.

The Path Forward Starts With the Right Partner.

Omega Systems' 2026 Healthcare IT Landscape Report reveals a sector under compounding pressure. The threats are not new. But the regulatory window is closing, the vendor attack surface is wider than most practices are monitoring, and the in-house security model that most rely on was never built for this moment.

The practices that will lead in the year ahead are the ones that stop treating these as parallel problems and build an integrated response – connecting security, compliance, vendor risk, and AI under a single managed program.

The decision that separates resilient healthcare practices from vulnerable ones is not about technology selection. It is about organizational posture – and who you trust to maintain it.

Cybersecurity done well is not a cost center. It is the foundation that makes everything else in a modern healthcare practice possible: safer patients, stronger compliance, and the confidence to grow.

01

Make Cybersecurity a Business Priority, Not a Technical One. Treat security investment as a core clinical and operational responsibility. The data is unambiguous: when leadership frames security as a cost center, every downstream decision reflects that.

02

Close the Vendor Visibility Gap. Confidence in a vendor network is not the same as visibility. Continuously monitor third-party connections and verify contracted security standards – because attackers are counting on the assumption that you won't.

03

Treat HIPAA Compliance as a Continuous Program, Not an Annual Event. The proposed 2026 HIPAA Security Rule mandates are specific, time-bound, and binary. The practices that will meet them are not doing more paperwork – they are operating under continuous monitoring, automated evidence collection, and expert guidance built in from the start.

04

Deploy AI With the Infrastructure to Support It. The revenue case for AI is real, and practice leaders know it. Capture it within a secure, auditable framework – because every new AI vendor is a new connection into your environment, and that connection carries the same risks as every other one documented in this report.

05

Stop Going It Alone. Security, compliance, vendor risk, and AI governance are not problems that scale with headcount. They require the kind of continuous, specialized expertise most practices cannot maintain internally.

Survey Methodology

These findings are based on an Omega Systems 2026 online survey of 200 healthcare business leaders in the United States. Titles included CEOs, CISOs, CIOs, CTOs, COOs, CFOs, and other IT leaders. Survey respondents work at organizations with 50 to 600 employees in the following healthcare sectors: medical practices and clinics, ambulatory care centers, specialty services (treatment centers, mental/behavioral health, etc.), and residential and long-term care facilities.

About Omega Systems

Omega Systems is a trusted managed service provider (MSP) and managed security service provider (MSSP) to healthcare organizations across the United States, including medical practices, ambulatory centers, and specialty care providers.
Founded in 2002, Omega combines managed IT services, cybersecurity operations, cloud infrastructure, and compliance support to help healthcare practices strengthen operational resilience, protect patient data, and meet evolving HIPAA requirements.

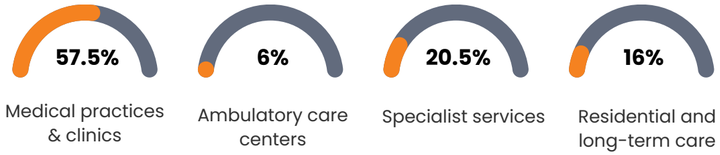
Through its security operations capabilities and integrated technology solutions, Omega helps healthcare providers modernize their IT and security environments while maintaining the visibility, control, and accountability required to safeguard sensitive health information and ensure continuity of care.

omega systems
technology managed

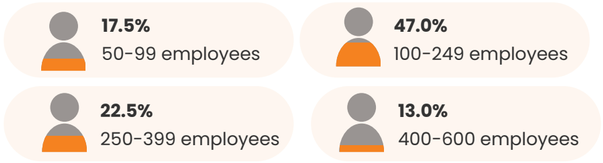
Appendix A

Demographics

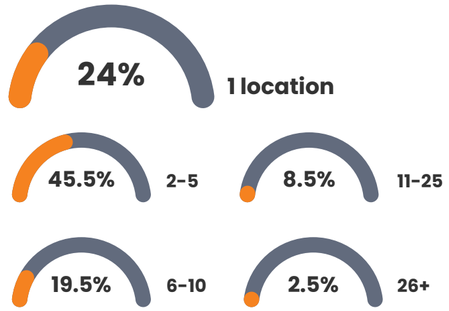
What sector does your healthcare organization operate in?



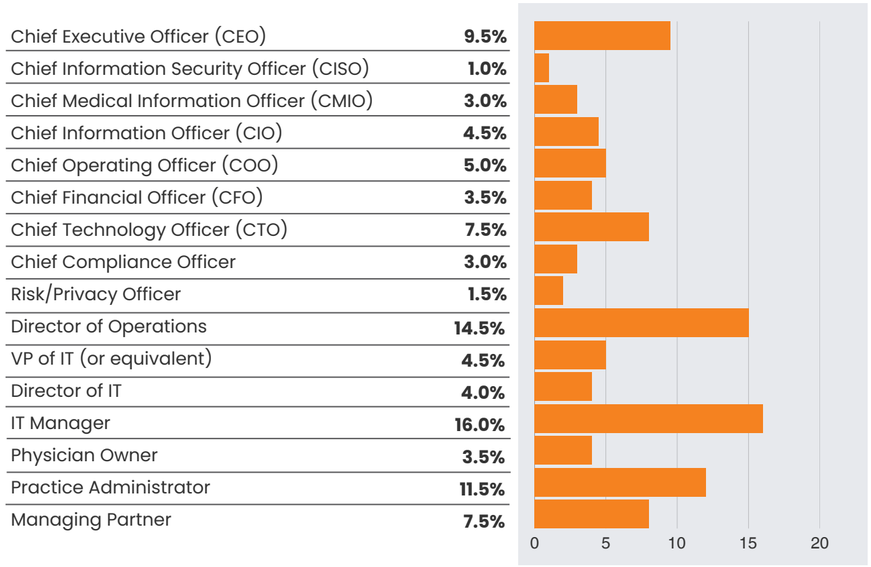
How many employees do you have?



How many locations does your practice operate?

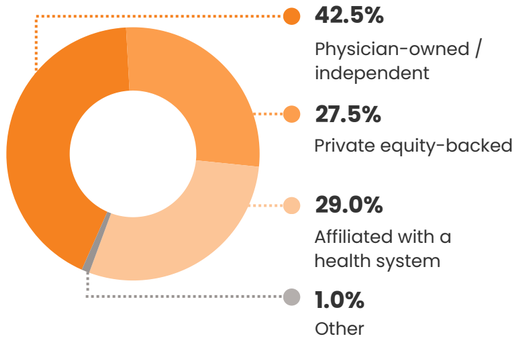


What is your job title?

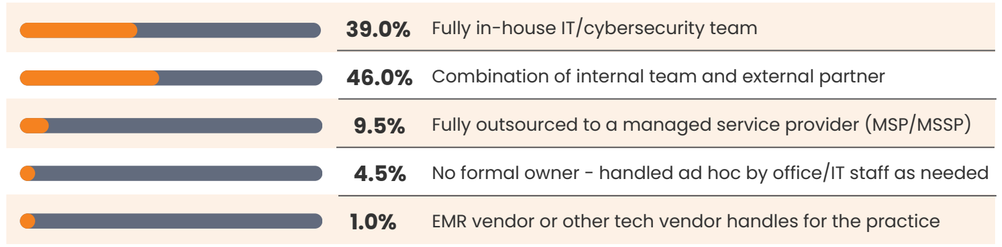


Chief Executive Officer (CEO)	9.5%
Chief Information Security Officer (CISO)	1.0%
Chief Medical Information Officer (CMIO)	3.0%
Chief Information Officer (CIO)	4.5%
Chief Operating Officer (COO)	5.0%
Chief Financial Officer (CFO)	3.5%
Chief Technology Officer (CTO)	7.5%
Chief Compliance Officer	3.0%
Risk/Privacy Officer	1.5%
Director of Operations	14.5%
VP of IT (or equivalent)	4.5%
Director of IT	4.0%
IT Manager	16.0%
Physician Owner	3.5%
Practice Administrator	11.5%
Managing Partner	7.5%

How would you describe your organization's ownership infrastructure?



Who is primarily responsible for managing cybersecurity and compliance at your practice?



39.0%	Fully in-house IT/cybersecurity team
46.0%	Combination of internal team and external partner
9.5%	Fully outsourced to a managed service provider (MSP/MSSP)
4.5%	No formal owner - handled ad hoc by office/IT staff as needed
1.0%	EMR vendor or other tech vendor handles for the practice