MarshMcLennan Agency

Healthcare Risk Report

Five forces reshaping the industry

Your future is limitless.℠

A business of Marsh McLennan

The cost of delivering care is growing faster than revenue.

Margins are shrinking. Demands are rising. For healthcare organizations, it's becoming more difficult to reconcile the two.

What started as a COVID-era squeeze has evolved into a long-term trend: the cost of delivering care is growing faster than the revenue it generates. This is now a top concern in every boardroom, and it's reshaping the risk environment.

When you follow the money, you see the pattern. **Cyber threats** are causing multi-million-dollar losses, and layered, often overlapping insurance policies. **Labor shortages** are pushing wages and reliance on agencies to unsustainable levels. **Regulatory enforcement** is ramping up as compliance resources are stretched thin. **Technology investments** promise long-term efficiency but require high upfront costs and can introduce new operational or liability risks. And **value-based care models**, while well-intentioned, expose providers to unpredictable reimbursement tied to outcomes they may not fully control.

What's more, many of these risks interact and compound in ways that amplify financial strain:

Technology investments + Regulatory complexity = Higher cost of compliance + Increased risk of error

Labor shortages + Contract staffing = Rising premiums + Staff-driven liability exposure

Cyber threats + Digital dependence = Operational disruption + Legal fallout + Insurance gaps

Value-based models + Workforce turnover = Missed outcomes + Unpredictable reimbursement

ALL OF THE ABOVE = Thinner margins + Increased difficulty securing affordable coverage

Today's healthcare leaders are managing margins and all the risks associated with—and caused by—costs. Individually, these risks are challenging. Together, they threaten the system's ability to sustain care.

How to read this report

This report is designed to help healthcare organizations navigate five of the most urgent financial and operational pressure points threatening healthcare stability today:

1. Cybersecurity threats
2. Labor shortages
3. Regulatory compliance
4. Technology disruptions
5. Value-based care models

Each section provides a detailed examination of a specific focus area, with clear connections to its impact on operational costs and margin preservation. To make this content as valuable as possible, we've included several navigation tools and visual cues to help you zero in on what's most relevant to your business.

Sector tags

At the beginning of each section—and throughout the text—these sector icons indicate where you can find risks and best practices specific to your sector. You can also use the matrix on the next page for a quick overview of where each threat is most relevant, emerging, or not currently significant.

Hospitals and physician groups

Acute care systems, health networks, physician groups, and large provider organizations

MedTech

Digital health, medical devices, biotech, and health tech companies

Long-term care

Senior living, skilled nursing facilities, rehab centers, and residential disability care

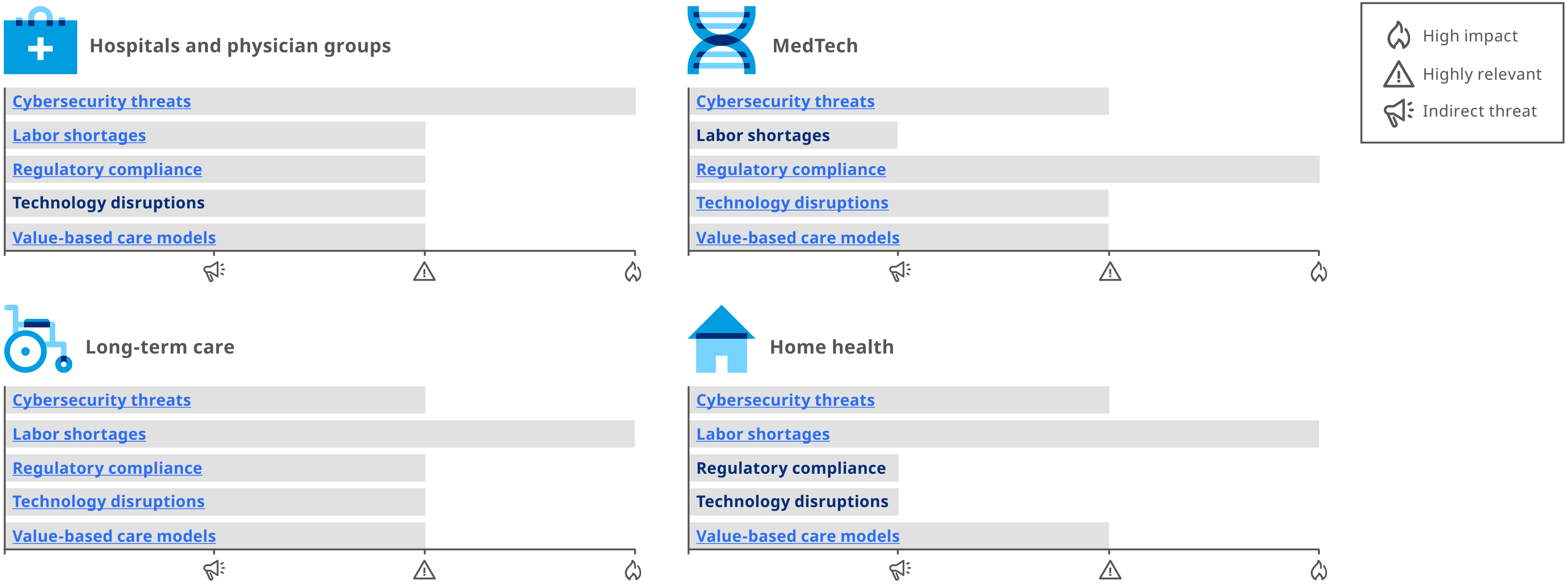
Home health

In-home care providers, mobile clinicians, and personal support services

Every focus area in this report is connected to the same root challenge: costs are rising faster than revenue. Be on the lookout for **cost driver callouts** so you can quickly see how these pressures are affecting your bottom line.

Risk by industry segment

Not every risk focus area applies equally across the healthcare ecosystem. Use this matrix for quick reference on how the industry's most pressing challenges affect four major healthcare sectors: hospitals, long-term care, MedTech, and home health.



Cybersecurity threats

The threat isn't new, but the frequency and severity are escalating.

Healthcare has been the costliest industry for data breaches since 2011, with an average breach cost of $9.77 million in 2024, significantly exceeding the $6.08 million average for financial services, which came in second. The reasons are well understood: patient records contain sensitive data, are difficult to replace, and are directly tied to high-stakes care delivery. What's changing is how the threat is evolving, how claims are surfacing, and where organizations find themselves increasingly exposed.

Ransomware remains the most common and disruptive cyber risk, but third-party cybersecurity incidents are surging. Rather than directly targeting a healthcare system, threat actors focus on vendors, billing firms, contractors, and other connected entities with weaker security. Long-term care facilities, in particular, are becoming unintentional gateways, seen not as the final target but as the easiest path. Residents may bring unsecured personal devices, and staff may not receive the same cybersecurity training or support as hospital teams.

Large physician groups face similar vulnerabilities. Their integration with major electronic health record platforms, high volumes of sensitive patient data, and reliance on third-party vendors make them equally attractive targets.

Hospitals and physician groups

$10 million was paid to resume cancer care. A ransomware attack encrypted an oncology practice's database. The breach cut off access to patient treatment plans. With tumors at the risk of progressing, the practice paid nearly $10 million to regain access and continue care.

Long-term care

Outdated vendor credentials could pose a security risk. A long-term care facility failed to completely remove a third-party vendor, leaving active credentials connected to its system and compromising its security. Hackers exploited the access point to navigate into an affiliated health system, triggering a broader breach.

Cyber risk now extends far beyond data theft, affecting clinical outcomes, reputation, and regulatory compliance. New litigation trends around pixel tracking and analytics tools expose organizations to unexpected class action lawsuits for collecting user behavior data without enough disclosure. These claims are rising quickly, and in response, several major cyber insurers have begun excluding this risk from standard policies altogether.

MedTech

Pixel tracking leads to wire fraud lawsuit. A direct-to-customer digital health company was sued after using website tracking tools without explicit user consent. The plaintiff's attorneys cited wire fraud and privacy violations, and the company's cyber insurer denied coverage due to a tracking-related exclusion.

Cyber incidents increasingly disrupt direct care by delaying treatment, disabling monitoring systems, and triggering high-dollar claims that **blur the lines between technical failure and clinical liability**. In some cases, what starts as a system outage can escalate into a medical malpractice suit, raising serious questions about how cyber and professional liability policies interact when patient safety is at risk.

Home health

Cyber failure results in birth injury. A cyberattack disabled fetal heart monitors in a hospital's labor and delivery unit. Staff missed signs of distress, leading to a birth injury. Although the root cause was technical, it led to the filing of a substantial claim as a medical malpractice case.

When cyber becomes a compliance risk

In 2024, False Claims Act settlements in healthcare reached $1.7 billion, with a significant share related to the integrity of electronic health records and billing compliance. While not always caused by cyberattacks, these settlements highlight a growing risk area. In an environment where care delivery relies on digital systems, the distinction between a technical failure and a federal investigation is becoming increasingly blurred.

Cost drivers

- **Ransomware payments** often reach millions of dollars and are made under pressure to resume care or avoid reputational fallout.
- **Operational downtime** can stop critical treatments and lead to costly service disruptions.
- **Legal defense and settlements** come from regulatory actions, pixel tracking lawsuits, and privacy violations.
- **Premiums** are rising, and **coverage exclusions** are becoming more common, especially for emerging risks like third-party exposure and web analytics tracking.
- **Overlap and confusion between cyber and malpractice coverage** can create gaps in protection when liability isn't clearly defined.

Managing the risk

Managing cyber risk means using technical controls, following best practices in risk management, and maintaining solid insurance coverage. As healthcare threats become more complex and costly, organizations should ensure they're not just protected on paper but ready in practice.

Start with strong coverage—but don't stop there.

Cyber insurance can be a vital financial backstop, but it's only effective if it matches the real threats your organization faces. Marsh McLennan Agency (MMA) can help clients get customized cyber coverage that fits their operational needs and risk profile. Remember, coverage should go beyond traditional data breach response and include:

- **First- and third-party protection**, including system restoration, business interruption, and liability to affected third parties
- **Ransomware and social engineering coverage**, paying special attention to sublimits and exclusions
- **Sector-specific underwriting** that reflects your record volume and system maturity
- **Alignment between cyber, crime, and professional liability policies** to close gaps between technical error, financial loss, and care delivery liability
- **Access to breach response partners** and clear protocols that meet real-world incident response demands

Build operational cyber resilience.

Insurance isn't a substitute for good cybersecurity practices. Organizations should focus on practical risk reduction to lower both the frequency and severity of issues:

- **Implement cybersecurity controls** like Marsh's top 12 cybersecurity controls, and work with knowledgeable partners to prioritize implementation based on your risk level and IT readiness.
- **Start the renewal process early** to engage with underwriters proactively. Working with advisors early in the renewal cycle gives you time to close gaps and strengthen your application profile.
- **Set up third-party onboarding and offboarding protocols** to reduce exposure from vendors. Long-term care and home health organizations are particularly at risk.
- **Get ready for holiday and off-hours exposure** by creating incident response plans that include off-shift coverage and clear escalation protocols.

Tap into specialized support.

Cyber threats are unique, and so is managing them. Work with risk management and insurance professionals who can:

- **Provide strategic guidance** throughout the policy lifecycle.
- **Support control implementation** and internal readiness.
- **Coordinate response and recovery** if an incident occurs.

Cyber threats are only becoming more sophisticated, but so are the tools and strategies we use to manage them. By taking a holistic, proactive approach, healthcare organizations can help protect both patient safety and financial stability.

Top 12 cybersecurity controls

Lacking essential cybersecurity controls can jeopardize your systems, reduce coverage, and raise costs. Our partners at Marsh recommend the following for your organization:

1. Multifactor authentication for remote access and admin/privileged controls
2. Endpoint detection and response (EDR)
3. Secured, encrypted, and tested backups
4. Privileged access management (PAM)
5. Email filtering and web security
6. Patch and vulnerability management
7. Cyber incident response planning and testing
8. Cybersecurity awareness training and phishing testing
9. Hardening techniques, including remote desktop protocol (RDP) protection
10. Logging, monitoring, and network protections
11. Replacement or protection of end-of-life systems
12. Vendor and digital supply chain risk management

MMA cyber advisory support

We support healthcare organizations with hands-on cyber risk consulting and policy placement. From systems assessments to vendor risk playbooks, our cyber resilience team helps clients enhance their security posture and improve their insurability. Embedded advisors work directly with IT teams to implement core controls and prepare for underwriting. If a breach occurs, our dedicated cyber claims advocates coordinate the right experts to reduce downtime, legal exposure, and recovery costs. Learn more.

Do you want to find out how protected your business is against cyberattacks?

Take the MMA Cyber Readiness Assessment.

Labor shortages

Care needs are rising, and capacity is running low.

Despite anticipated growth in the overall workforce, the U.S. healthcare system is expected to face a shortage of over

100,000

workers by 2028.

The issue isn't just headcount—it's who's leaving, who isn't entering, and where the biggest gaps appear. From registered nurses to home health aides, the labor shortage is straining care delivery, reshaping budgets, and threatening the long-term viability of many healthcare organizations.

Burnout is driving exits. Even as the immediate pressures of COVID ease, burnout remains a persistent threat, especially for nurses and frontline support roles. In 2022 alone, over 100,000 registered nurses (RN) left the workforce due to stress, burnout, or early retirement. A 2023 survey found that half of U.S. clinicians are considering leaving their jobs within the next 2–3 years, and a third are thinking about leaving healthcare altogether.

Hospitals and physician groups + long-term care

Hospitals, physician groups, and long-term care facilities are experiencing a cycle of attrition. Short staffing leads to stress, which leads to more exits and deepens the shortage. Physician staffing shortages are especially pronounced in rural areas. One large provider group described a doctor commuting from Chicago to northern Wisconsin to cover multi-day shifts. This expensive, unsustainable solution highlights the growing difficulty of attracting physicians to underserved regions.

Compensation and competition are squeezing margins. The labor shortage isn't just about people leaving. Organizations also struggle to attract new workers. Low-wage roles, such as nursing assistants and home health aides, make up a large part of the healthcare workforce, but many earn less than $15 per hour on average. In states like New York and New Jersey, workers are crossing state lines to find better pay, which is increasing local shortages.

Home health

In home health, employers aren't just competing with hospitals but also with other industries for entry-level workers. Personal safety risks, long commutes, and unpredictable home conditions make it a tough sell.

Employees expect more than just pay. They want flexibility, growth, and support. Mental health, financial wellness, and a meaningful culture are top priorities, especially for younger generations. Total rewards strategies, including personalized benefits and financial education, are key for employers hoping to retain and attract top talent.

The healthcare workforce is aging. At the same time, the "silver wave" continues to surge as more seniors enter care facilities or require in-home care, while fewer younger professionals are choosing careers in these fields. This demographic shift presents ongoing challenges for staffing, retention, and workforce planning in healthcare.

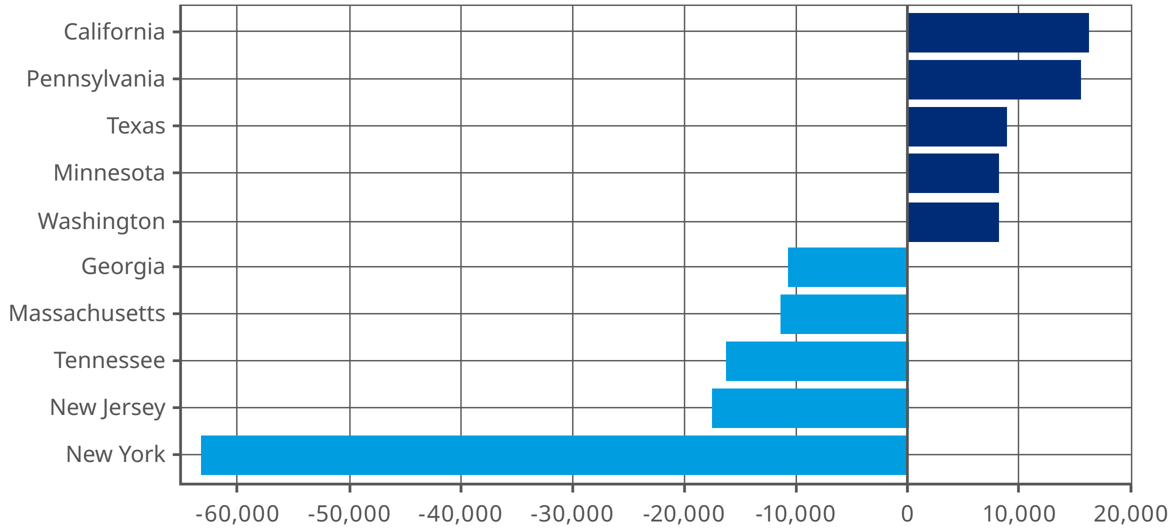
Long-term care

Senior living facilities face a double challenge: rising demand and a shrinking pool of qualified workers. In many cases, generational wealth isn't keeping pace. More patients rely on Medicaid, putting even more stress on budgets and staffing. Burnout is even harder to recover from. Workers often move to higher-paying or less emotionally demanding jobs, leaving facilities to fill gaps with agency staff or less experienced hires.

State-by-state labor projects

Workforce shortages aren't distributed evenly across the U.S., and the effects on talent strategy, compensation, and care vary widely by location. Mercer's Future of the U.S. Healthcare Industry report offers the following insights into the healthcare labor market.

The top five projected shortage and surplus states



13 **states** are expected to meet or exceed the demand for nursing assistants.

18K New York, New Jersey, and Connecticut are projected to fall short by over **18,000 home health aides** combined.

Nurse practitioner shortages are expected, even in states like California and Texas, which are considered surplus.

Cost drivers

- **Premium pay for contract labor**, with travel nurses often costing two to three times more than full-time staff
- **Turnover-related expenses**, including recruitment, onboarding, and training for high-churn roles like RNs and nursing assistants
- **Wage pressure** driven by competition with other healthcare providers and non-healthcare employers for entry-level talent
- **Increased liability and abuse/ molestation premiums** in long-term care and home health due to staffing instability and inconsistent caregiver assignments
- **Productivity losses and absenteeism linked to burnout**, especially among frontline clinical and caregiving roles
- **Higher Medicaid use among aging patients**, reducing reimbursement rates while staffing costs continue to rise

Managing the risk

Labor shortages are a widespread problem. However, a proactive workforce strategy can help healthcare organizations manage costs, enhance employee retention, and remain competitive in a tightening market. The most successful organizations will align pay, benefits, and culture to support their people and plan for long-term stability.

Benchmark compensation with benefits.

Labor markets are local. Use data-driven benchmarking to make sure your pay, PTO, and benefits programs match your industry, region, and competitors:

- **Look beyond wages** to assess total rewards like 401(k) matching, health benefits, and professional development opportunities.
- **Monitor other shifts**, such as cost of living, migration patterns, and pay scales in related sectors, to prevent unexpected talent loss.

Invest in retention.

Retention strategies don't need to be elaborate to be effective. Small, meaningful investments can boost morale and lower turnover:

- **Prioritize strong hiring practices** that include background and reference checks to ensure the right fit from the start.
- **Support employees** with mental health resources, flexible schedules, and financial education.
- **Explore referral and retention bonuses** as low-cost ways to reward loyalty and grow your talent pool.
- **Address burnout directly** with targeted well-being programs and workload management strategies.

Personalize and segment your benefit strategy.

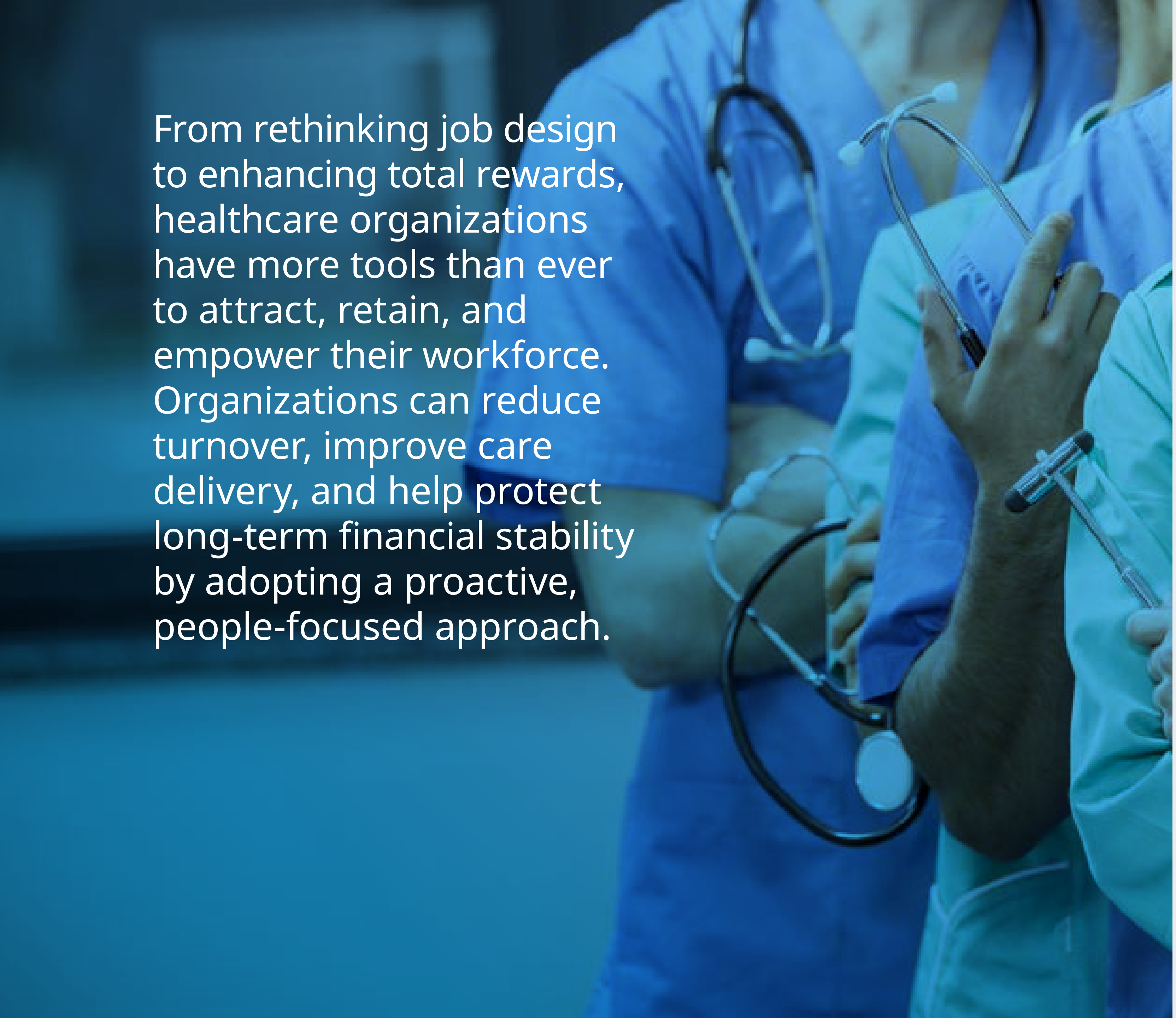
Not all employees value the same benefits. Tailored benefit design and delivery can make programs more impactful:

- **Use workforce data** to identify benefit preferences across roles, generations, and locations.
- **Segment communications** to help employees understand and engage with the programs most relevant to them.
- **Offer opt-in flexibility** that lets employees choose what works for them.

Build internal pipelines.

Workforce development takes time. Health systems should cultivate talent from within and nurture external relationships.

- **Partner with local schools and certification programs** to create specific pathways for roles.
- **Support mentorship, onboarding, and upskilling initiatives** that help junior talent move into hard-to-fill positions.



From rethinking job design to enhancing total rewards, healthcare organizations have more tools than ever to attract, retain, and empower their workforce. Organizations can reduce turnover, improve care delivery, and help protect long-term financial stability by adopting a proactive, people-focused approach.

MMA solutions for workforce strategy

We help healthcare organizations strengthen their workforce with data-driven strategies and tailored benefits programs. Our integrated approach combines workforce analytics, strategic plan management, and targeted communications to align your benefits with employee needs and business goals. Tools like Planning & Analytics for Total Health (PATH) turn data into insight, while Workers' Health 360® connects claims, health, and absenteeism trends to identify risk early.

To enhance employee support, we offer financial wellness coaching through MMA Prosper Wise, pharmacy cost management via Rx Solutions, and a wide range of voluntary benefits that bring flexibility and personalization to your total rewards package.

We also help simplify access with mobile-friendly platforms and engagement strategies that ensure employees understand and value your benefits, no matter where or how they work.

Regulatory compliance

A moving target with rising stakes

U.S. healthcare organizations collectively spend approximately

$39B

on administrative activities

related to regulatory compliance per year. As one of the most regulated industries in the country, healthcare organizations must constantly navigate a complex and changing set of rules. From False Claims Act settlements to evolving FDA enforcement, regulatory pressures are ever-present and increasingly costly. As innovation and consolidation reshape healthcare, organizations are working to meet compliance demands without compromising care quality and financial stability.

The rules keep shifting for MedTech.

Pixel tracking lawsuits and consent violations have triggered class actions and policy exclusions. Corporate practice of medicine enforcement is picking up, especially for digital-first providers working across state lines. Although there are hopes for less strict enforcement under the current administration, the regulatory bar for innovation remains high.

GLP-1 compounding creates a regulatory storm.

After the FDA lifted its declaration of shortage for GLP-1 drugs, compounding pharmacies continued to manufacture and sell alternatives, often by modifying the ingredients. While smaller players stepped back, larger compounders kept producing. Now, pharmaceutical giants are suing for patent infringement. The situation has revealed considerable regulatory and legal risks, with unclear FDA guidance, patchwork enforcement, and rising litigation costs, all while demand for the drug continues to surge.

Tariffs add even more volatility to the mix. As supplier costs rise, some overseas partners close, leaving companies with undelivered orders and unpaid invoices. Demand for trade credit insurance is growing, but market capacity is shrinking. Protecting cash flow has become just as important for MedTech firms as navigating compliance.

Large institutions feel the weight of audits, mergers, and compliance fatigue.

Scrutiny under the False Claims Act remains high, and antitrust reviews complicate mergers and acquisitions. Compliance demands continue to take up time and resources, often pulling them away from direct patient care. Even smaller systems now require dedicated regulatory staff just to keep pace.

Multi-state physician groups encounter heightened regulatory risk.

As they grow through mergers or expand telehealth offerings across state lines, multi-state physician groups face increased regulatory risk. While corporate practice of medicine laws aim to protect clinical decision-making from business influence, these laws can vary significantly by state and are often complex to navigate. As enforcement intensifies, the risk of fines, licensing challenges, and legal scrutiny also rises.

Senior living is facing increased scrutiny as consolidation in the industry continues.

Growth backed by private equity has attracted regulatory attention. As facilities scale, concerns about the quality of care, staffing levels, and reliance on Medicaid also grow. Proposed mandates and shifting reimbursement models are increasing compliance risk, and many providers are now caught between policy demands and operational challenges.

Cost drivers

- **Fines and settlements from state and federal enforcement**, often in the tens of millions
- **Legal costs** tied to regulatory defense, internal investigations, and whistleblower claims
- **Operational disruptions** from audits, compliance reviews, and mandated process changes
- **Margin loss** from supply chain fallout (e.g., GLP-1 drug restrictions, tariff volatility)
- **Higher spending** on regulatory staff, tools, and training, especially for smaller organizations scaling up

Managing the risk

Managing regulatory compliance starts with building structural safeguards and encouraging cultural accountability. The most successful healthcare organizations strike a balance between standardization and input from frontline staff, developing systems that can adjust to the growing complexity of care delivery.

Build a proactive compliance infrastructure.

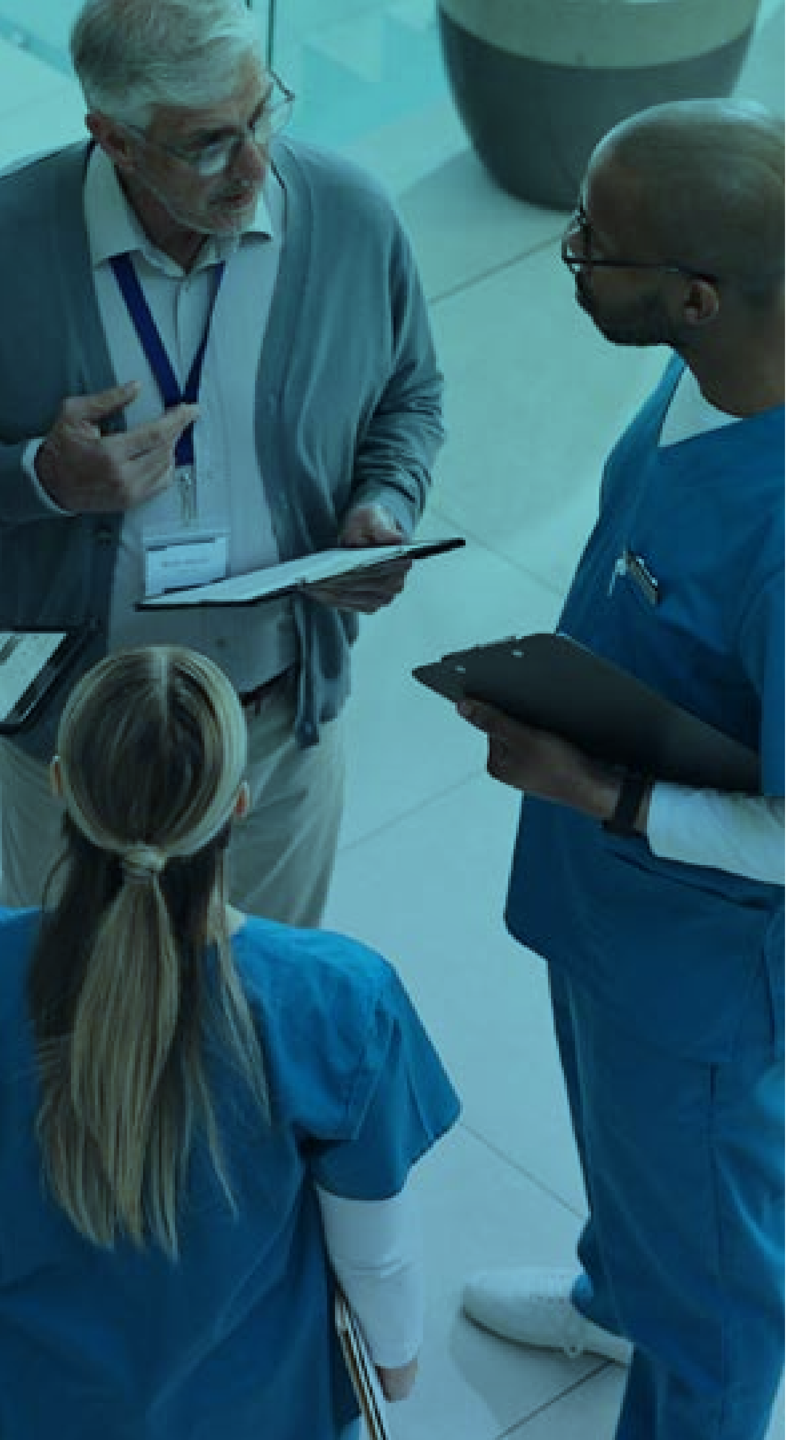
Compliance isn't just a job for one person or one department. It should be part of the entire organization and regularly tested.

- **Adopt and adjust corporate compliance standards.** Make sure they're tailored to your business model, state requirements, and specific risks in your sector.
- **Conduct regular mock surveys.** Prepare for state and federal audits by testing compliance procedures before an official review.
- **Form regulatory working groups that include frontline staff.** Employees doing the work should have a say in policy development. They're closest to the pain points and can best identify practical solutions.
- **Embrace feedback from the ground up.** Compliance frameworks that don't reflect clinical realities are rarely effective. Engage staff early and often.
- **Invest in education and technology.** Smart systems and well-designed training can lower compliance costs and reduce the burden on clinicians. Use AI to simplify documentation and reporting, offer targeted training for different roles, and ensure your compliance team has the resources to meet changing oversight demands.

Monitor evolving risks.

Regulatory pressure is dynamic, and today's gray areas can turn into tomorrow's liabilities.

- **Stay ahead of FDA enforcement.** Even minor product alterations can trigger new clearance requirements for MedTech and biotech firms, especially for drugs under active scrutiny.
- **Watch for antitrust activity.** As hospitals and insurers consolidate, merger activity may lead to more thorough regulatory reviews. Legal and compliance teams need to be engaged from the beginning.
- **Assess trade risks and credit exposure.** Changes in tariffs and global supply instability can threaten receivables and increase risk. Trade credit insurance may be a helpful tool for companies facing potential customer and supplier defaults.



Building a broader financial safety net

In today's unpredictable environment, financial protection requires more than one policy. Here are three often-overlooked but increasingly essential types of coverage that can help boost financial resilience.

Trade credit insurance helps protect your organization when customers or suppliers fail to pay for goods and services, whether due to insolvency, default, or political risk. This protection is becoming increasingly essential for MedTech and health systems sourcing materials globally.

Use it to:

- Protect high-value receivables.
- Strengthen balance sheets.
- Secure financing with insured assets.
- Reduce risk from customer or supplier insolvency.

Medical professional liability insurance shields healthcare providers and organizations from claims of negligence, treatment errors, or diagnostic mistakes that result in patient harm. This coverage is tailored for healthcare-related risks and is frequently necessary for regulatory compliance.

Use it to:

- Defend against treatment and diagnostic error claims.
- Cover legal costs related to patient harm allegations.
- Protect clinical decisions from regulatory exposure.
- Meet compliance expectations for coverage.

Errors and omissions (E&O) is traditionally associated with non-clinical claims and is intended to cover third-party financial losses resulting from errors in business services or administrative decisions. This can include technology-related failures in MedTech or digital health that lead to patient harm.

Use it to:

- Cover legal costs from billing or documentation errors.
- Protect against denial-of-service claims.
- Address compliance-related financial exposures.

Technology disruptions

The use of AI is creating wider coverage gaps.

Technology can change how healthcare is delivered by using ambient listening, digital diagnostics, wearable monitors, and AI-assisted scheduling.

However, as new solutions emerge, healthcare organizations face a tough reality: innovation is expensive, disruptive, and outpacing most organizations' ability to adopt it safely.

However, many organizations struggle to modernize their systems due to limited capital, legacy constraints, and resource gaps. Without the ability to upgrade their tech stacks or invest in improvements, providers are stuck with outdated billing systems or overly dependent on a single vendor. When third-party systems go down, the ripple effects can stall operations across the continuum of care.

At the same time, MedTech and digital health companies are racing to be disruptors. Generative AI scribes, AI-assisted diagnostics, and automated appointment scheduling are just the beginning. As these technologies edge closer to clinical decision-making, the line between tech provider and healthcare provider is blurring, raising questions about accountability, standards of care, and insurance coverage.

90% **of health system leaders say digital transformation affects their strategy this year.**

Long-term care

Senior living facilities are exploring AI solutions to reduce falls and manage chronic conditions, but using these tools brings risk. In environments with limited staff and no on-site doctors, vicarious liability remains a serious concern if AI tools are seen as providing care.

MedTech

AI nurses and diagnostic tools could soon face lawsuits not as products but as providers, triggering malpractice-style litigation. Without clear regulatory or insurance guidelines, healthcare organizations may unknowingly expose themselves to coverage gaps.

So far, few insurance carriers offer dedicated AI coverage. The early solutions are usually bundled into technology E&O or cyber policies, sometimes with endorsements for AI services. Still, gaps remain, especially when tools intersect with patient care or could be perceived as practicing medicine. The risk isn't that AI will fail; it's that AI will succeed without a clear plan for where liability lies, and the fear is that there won't be any clinical oversight of the AI.

Cost drivers

- **High upfront investment** needed for system-wide adoption, integration, and training
- **Operational downtime** during tech transitions or third-party outages
- **Legal liability** from AI misdiagnosis, errors, or care missteps that may lead to malpractice territory
- **Coverage gaps arise** when AI tools or tech platforms are not clearly included in existing E&O, cyber, or professional liability policies

Managing the risk

As healthcare organizations speed up digital transformation, success relies on creating the right infrastructure, maintaining oversight, and preparing staff for meaningful adoption.

Start with governance.

- **Define who makes decisions** about AI and automation.
- **Align roles and responsibilities** across clinical, IT, and compliance teams.

Implement with purpose.

- **Prioritize tools** that reduce friction, enhance care, or support staff—not just innovation for its own sake.
- **Focus on outcomes**, not just features.

Train and test your teams.

- **Prevent alert fatigue** and system errors with targeted training.
- **Clarify when and how to respond** to tech-generated insights or prompts.

Audit your tech stack.

- **Evaluate third-party tools** for security, coverage, and readiness for failover.
- **Look for single points of failure** or unclear accountability in contracts.

Plan for downtime.

- **Incorporate all critical systems**, including external platforms, in business continuity planning.
- **Ensure staff know how to operate manually** when needed.

Technology can create real efficiency, but only if implemented with purpose and backed by operational readiness. Without the right strategy, even well-designed tools can introduce new risks and hidden costs.

How to coordinate coverages to cover technology risk

The boundary between clinical care and technology is only getting blurrier. That's why insurance strategies need to evolve with innovation. Traditional malpractice and cyber policies may not provide enough protection on their own. A single care decision could now be influenced by software, highlighted through automation, and carried out by a clinician.

MMA helps organizations navigate this convergence by structuring coordinated coverage across technology E&O, medical professional liability, and cyber. This starts with clearly understanding how your tech is used in clinical workflows, then aligning coverage to match real-world risk.

"Future disruption" or just the future?

AI and automation aren't just disrupting healthcare; they're becoming part of it. The question isn't whether organizations will use AI, but how, where, and with what protections. The fastest-moving technology isn't always the safest, and being too early or late can create risk. Now is the time to:

- Map how AI is used across clinical and non-clinical workflows.
- Identify where oversight is human versus automated.
- Check if your E&O, cyber, and professional liability policies are aligned.

Value-based care models

Healthcare reimagined—but execution is everything.

At its core, value-based care addresses healthcare's biggest financial challenge: the cost of delivering care is rising faster than the reimbursement received. Hospital margins are under pressure from all sides: labor costs, flat government payments, and rising expenses for drugs, supplies, and insurance.

Value-based care offers a path to sustainability by rewarding outcomes rather than volume. When providers can keep patients healthier and out of the hospital, they can lower preventable costs and share in the savings.

But implementation is complex. Models such as bundled payments, capitation, Medicare Advantage, and shared savings all require a new approach to care that focuses on data, coordination, and managing population-level risk. Shifting from a fee-for-service model means taking on more financial risk, investing in infrastructure, and redesigning care around outcomes rather than visits.

Hospitals and physician groups are at the center of value-based transformation, each playing essential but distinct roles in managing population health and financial risk. They are also the most financially vulnerable. Many hospitals already operate on razor-thin margins. Value-based models may help stabilize revenue through shared savings, but only if hospitals can invest in data infrastructure, effectively manage care coordination, and navigate the risks tied to downside contracts. While physician groups are often more agile, they may take on significant downside risk without the financial protections hospitals typically have in place.

As digital health and MedTech companies take on full-risk contracts, build their provider networks, and use data to drive outcomes, many are stepping into roles that carry clinical and financial liability. Without dedicated managed care or stop-loss coverage, these organizations may not be ready for the consequences of failed interventions or poor outcomes.

Long-term care and home health providers are essential in value-based models, as they help prevent costly hospitalizations. But success relies on their ability to manage complex populations with limited resources. These providers need to show outcomes, track risks, and respond proactively to early warning signs while adapting to changing reimbursement models.

When profit leaves the building

Hospitals are losing some of their most profitable services to outpatient surgery centers. From GI procedures and orthopedics to LASIK and urology, these centers work more efficiently and often have lower infection rates, shorter recovery times, and reduced costs—all factors that value-based care rewards. But for hospitals, this shift means:

- Fewer commercial insurance reimbursements for high-margin procedures
- A shrinking ability to offset losses from Medicaid, Medicare, and uncompensated care
- Increased pressure to optimize their service mix and prove value in every line of care

Cost drivers

- **Reimbursement misalignment** where the costs of care exceed payments, particularly in high-acuity or Medicare/Medicaid-heavy populations
- **Data and technology investments** needed to track, analyze, and act on outcomes in real time
- **Downside risk exposure** for providers taking full or partial capitation without financial protection
- **Operational overhead** for managing service mix, payer mix, and case mix across complex populations
- **Patient noncompliance**, where even well-structured models falter if individuals don't follow care plans, take medications, and attend follow-ups

Managing the risk

Value-based care can be transformative when risk is understood, managed, and insured. Success requires a coordinated strategy, accurate data, and careful insurance placement.

Understand your exposure.

If your organization processes claims, makes clinical decisions using software, or has at-risk contracts for specific patient populations, your exposure likely goes beyond traditional E&O. You may need:

- **Managed care E&O** to cover errors in claims processing, denial of services, or treatment delays
- **Technology E&O** if software is making or influencing care decisions
- **Downside risk insurance or provider excess loss coverage** to protect against catastrophic claim overruns in capitated or shared savings arrangements

Coordinate your coverage.

When tech, care, and finance are interconnected, gaps can form. This is especially true if managed care E&O excludes tech-related claims, and vice versa.

Build a smart care model.

It's not just about managing risk. Providers must optimize:

- **Payer mix:** Who pays for your care and at what rate?
- **Service mix:** Where and how do patients receive care—hospital, outpatient, in-home?
- **Case mix:** Accurately document patient acuity to receive full reimbursement.

Leverage your data.

Outcomes start with insight. Use patterns to understand:

- Which patients are at the highest risk and why?
- How can early interventions reduce acute incidents?
- How to document, analyze, and share success with payers and patients?

Effective population health management involves outreach, education, care coordination, and sometimes logistical interventions, such as delivering water when temperatures rise, proactively scheduling pre- and post-appointments, or providing monitoring devices. The better you manage patient health, the more financially sustainable your model becomes.

How MMA supports value-based care strategy

Our consulting services are designed to help you align operations, data, and insurance strategy so that value-based care becomes more than a reimbursement model—it becomes a performance advantage.

Here's how we can help:

- **Data-driven care design:** We collaborate with clients to examine payer, service, and case mix, ensuring your contracts, delivery models, and documentation align with reimbursement strategies and patient outcomes.
- **Risk assessment and coverage coordination:** From managed care E&O to stop-loss protection, we help you find gaps in your insurance portfolio and coordinate policies across care delivery, tech platforms, and population health management.
- **Outcome-based performance modeling:** Our teams help evaluate readmission rates, care gaps, and follow-up patterns, then build models that improve results and support shared savings.
- **Domestic network and benefit optimization:** For health systems managing their populations, we consult on proprietary networks, pharmacy strategies, and tiered benefit plans that improve outcomes and lower costs.
- **Proactive intervention strategy:** Whether it's designing heatwave outreach or chronic care pathways, we help translate your data into action before a health event becomes a high-cost claim.

When the cost of care outpaces revenue

The cost of delivering care continues to rise—encompassing labor, supplies, technology, and insurance—while reimbursement remains flat. Whether you're managing a nonprofit hospital, a growing senior care network, or a tech-enabled care platform, the challenge is the same: making care sustainable under mounting financial pressure. Every dollar counts, and every operational decision has a ripple effect.

At MMA, we help healthcare organizations manage these growing pressures through smarter cost projections, better-aligned benefits, and integrated insurance strategies. From regulatory liability and workforce planning to AI governance and medical professional liability coverage, we focus on helping clients protect their mission and their margin.

Reach out to a specialist today to learn more about how to manage your risk.

About Marsh McLennan Agency

Marsh McLennan Agency (MMA) provides business insurance, employee health & benefits, retirement, and private client insurance solutions to organizations and individuals seeking limitless possibilities. With 15,000+ colleagues and 300+ offices across United States and Canada, MMA combines the personalized service model of a local consultant with the global resources of the world's leading professional services firm, Marsh McLennan (NYSE: MMC).

01_1633478557_0725

Business Insurance
Employee Health & Benefits
Private Client Services
Retirement & Wealth

MarshMcLennan Agency

A business of Marsh McLennan