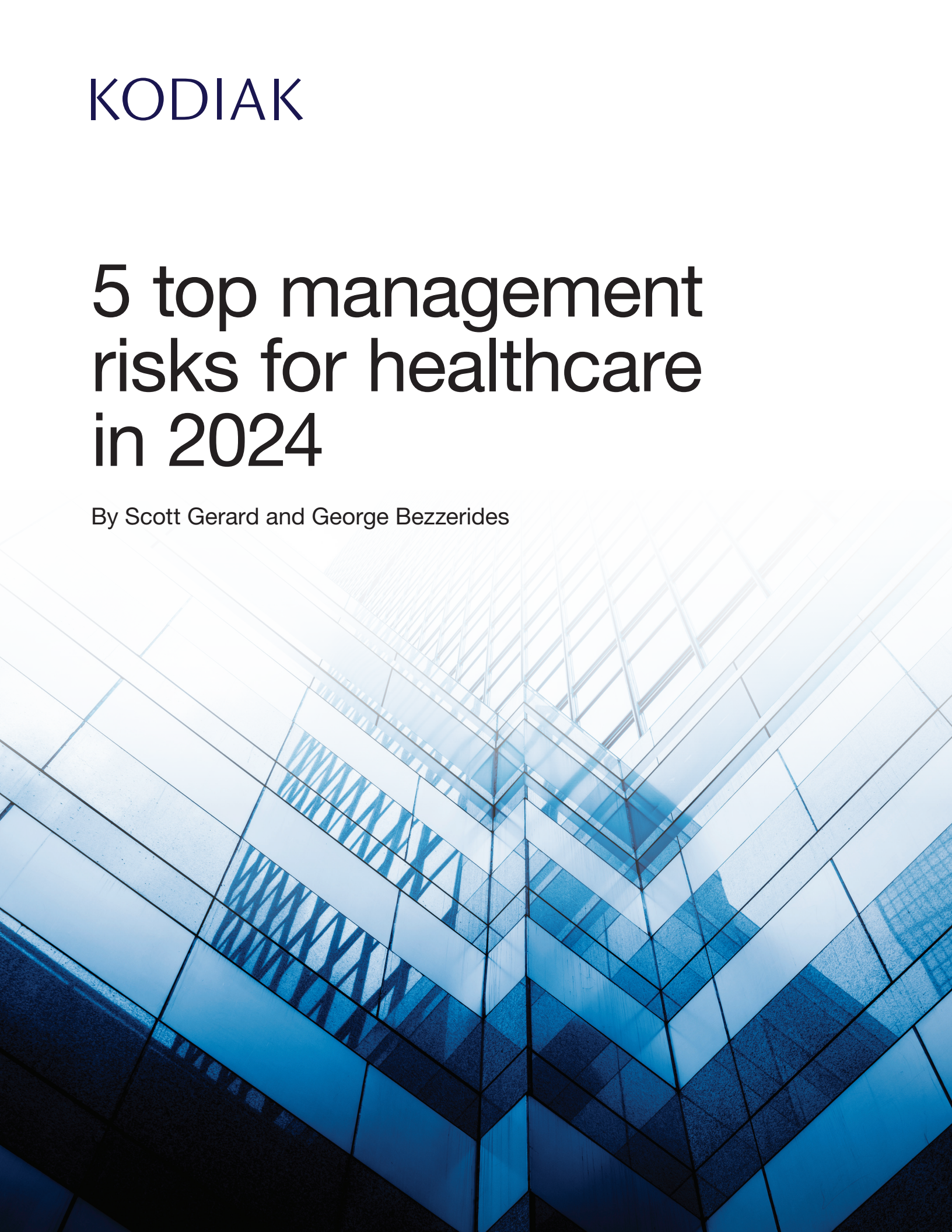
KODIAK

5 top management risks for healthcare in 2024

By Scott Gerard and George Bezzerides



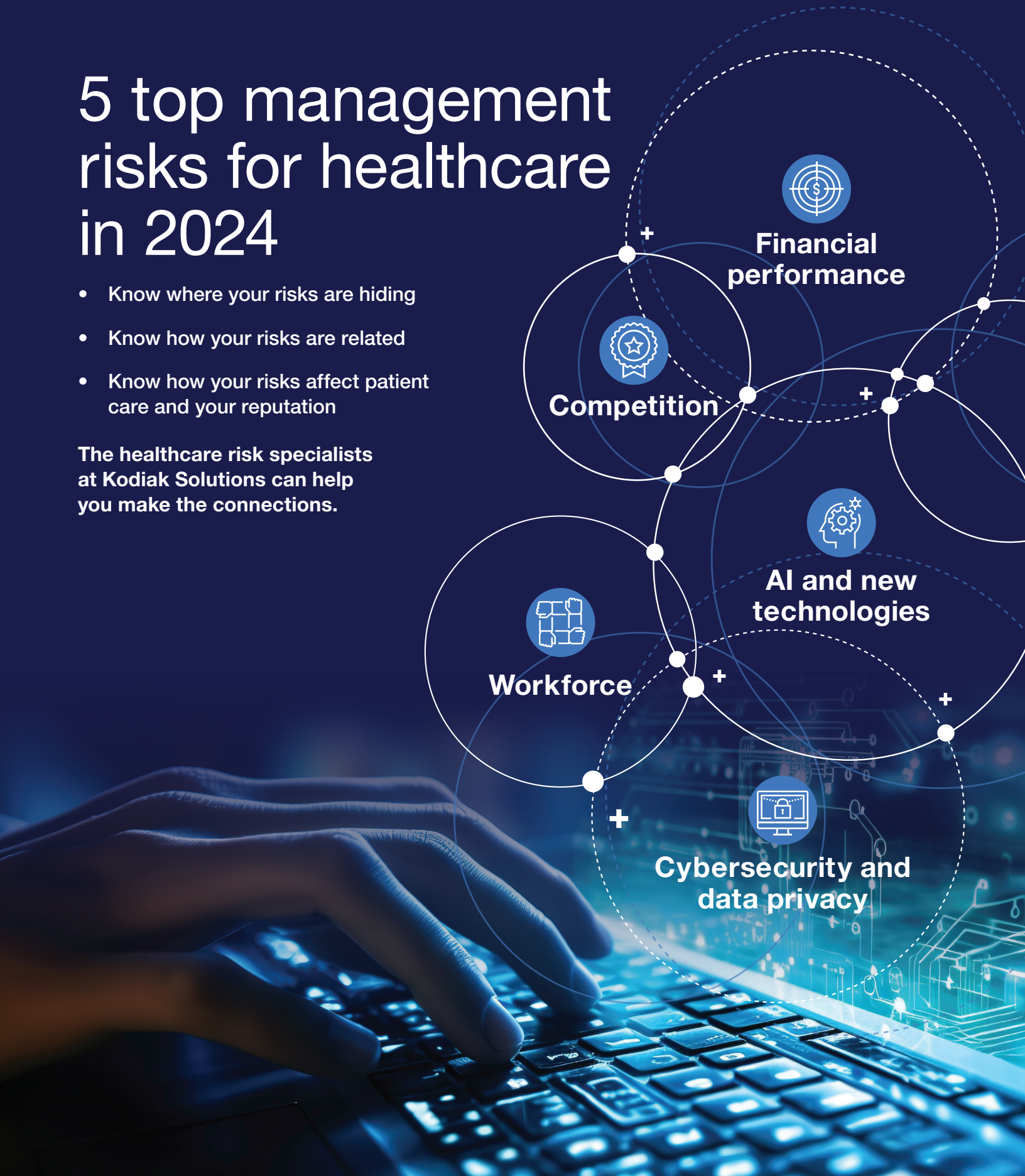
Healthcare provider organizations face difficult choices about where to best allocate their financial capital and human resources. While trying to minimize undue risk exposure and enhance return on mitigation efforts, organizations are confronting an inflationary economy made worse by increased competition, more frequent cyberattacks, and shortages of clinical, IT, and risk professionals.

A successful decision-making process begins by knowing where risks are hiding, how various risks are interconnected, and how these risks affect an organization's patient care capabilities and reputation.

5 top management risks for healthcare in 2024

- Know where your risks are hiding
- Know how your risks are related
- Know how your risks affect patient care and your reputation

The healthcare risk specialists at Kodiak Solutions can help you make the connections.



Introduction

Kodiak Solutions defines a risk area as anything that might impede a healthcare organization's ability to achieve its goals in critical areas, like:

- Patient care
- Regulatory compliance
- Operations
- Strategic growth
- Financial performance

To manage an environment of increasing risks and limited resources, healthcare internal audit and compliance departments must align their risk assessments and audit work plans to areas most vital to achieving the strategic goals and business objectives of their organizations. This risk-based approach prioritizes areas of highest risk and suggests that providers spend less effort, if any, on low-risk areas.

The better the alignment between the internal audit and compliance plans and the most critical risks to the organization, the greater the return on risk generated for the organization's internal audit and compliance investment.

Kodiak has identified five top management risk areas facing healthcare organizations that internal audit and compliance leaders should assess and keep on their radar screens as they plan for 2024. The five top management risks, in alphabetical order, are:

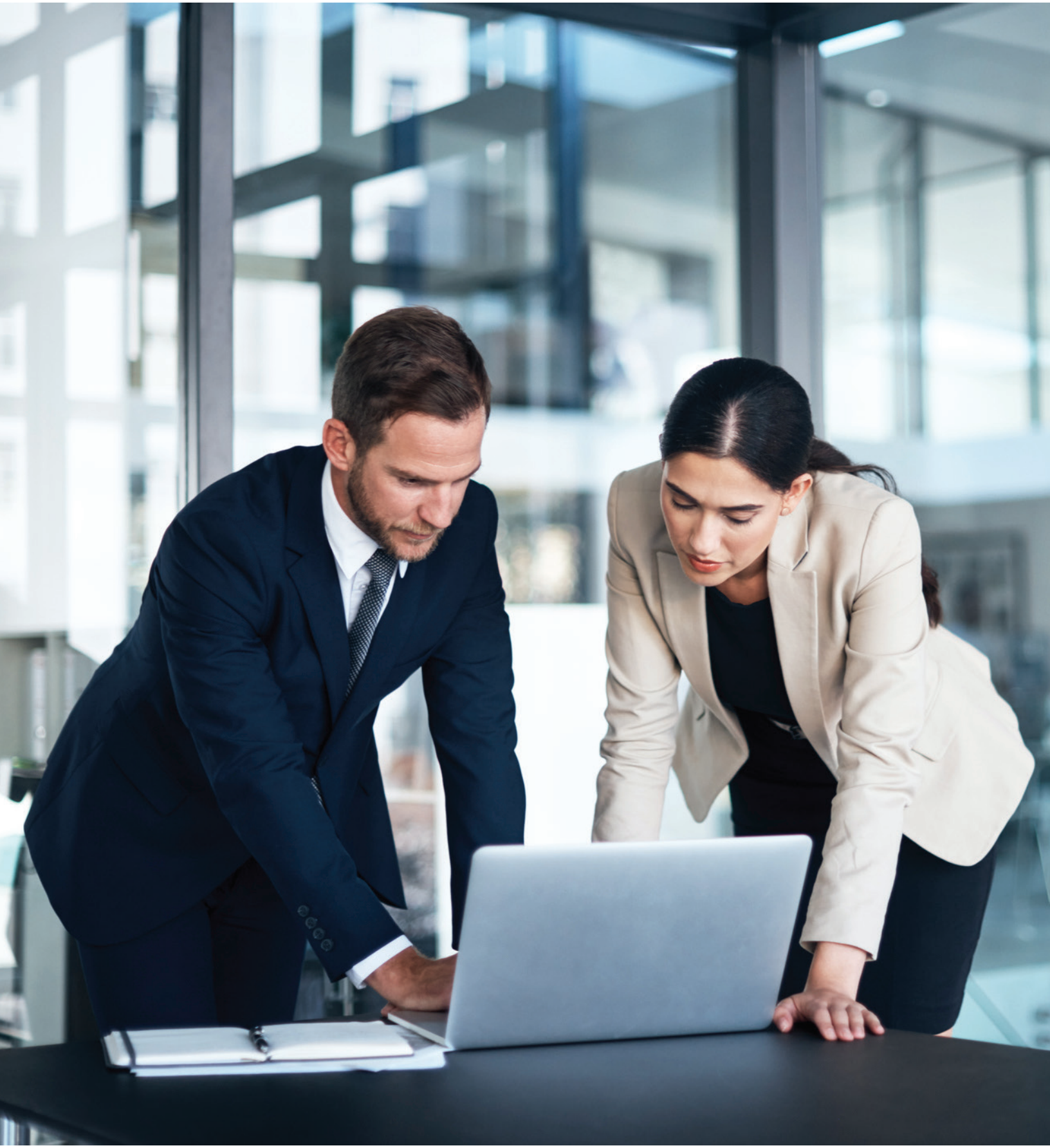
- Artificial intelligence (AI) and new technologies
- Competition
- Cybersecurity and data privacy
- Financial performance
- Workforce

These five top management risk areas were identified based on input from:

- Executive management and board members at many of the largest U.S. health systems
- Risk assessments conducted by Kodiak in 2023 at hundreds of hospitals, health systems, medical practices, and other healthcare provider organizations

Every healthcare organization is different. A top risk area for one healthcare organization might not be a risk for another organization.

It is also important to note how these five top risk areas interconnect and affect patient care and an organization's reputation. The report also includes a recommended reading list of materials that support the identification and mitigation of each of the five risk areas.



1. Risk area: AI and new technologies

The benefit to the healthcare industry from using generative AI, machine learning (ML), and other new technologies can be significant over the next several years. Though the industry has already been using such smart technologies for years, as more use cases are developed and AI and other tools become more accepted across the industry, healthcare providers could enjoy:

- Greater employee and process efficiencies, such as automated clinical documentation and confirmation of insurance coverage
- Faster and more accurate diagnosis leading to enhanced treatment protocols and better clinical outcomes
- Improved patient and customer experience in areas such as enhanced appointment scheduling and customer service calls

At the same time, the substantial benefits will create new risks for those using new and innovative technologies. Here are some new risks associated with AI and new technologies:

- Training of AI and ML models involves enormous amounts of data that must be used and stored. Much of the data could be protected health information (PHI) coveted by cybercriminals and subject to HIPAA and state privacy regulations. Breaches of AI-related data could subject a healthcare organization to significant financial penalties and reputational risk.
- Bad actors inserting bad data into AI models increases risks of corrupting the resulting data-driven insights, making them potentially dangerous if used for patient care.
- AI algorithms carry the potential for bias and other limitations.

- Patients might lack confidence in the use of new technologies.
- AI could be used for malicious purposes. Bad actors have accessed widely used AI to create phishing emails that are well written and, as a result, are more likely to deceive the reader.

Other risk areas affected

Cybersecurity and data privacy. Along with the many benefits of AI and new technologies, healthcare organizations need to be aware of several security and privacy risks. As organizations obtain and store more PHI and sensitive patient data, the risks surrounding data breaches increase as these organizations become more valuable targets. Healthcare organizations also must secure their data effectively, as these systems could be targeted with ransomware, theft, or inappropriate changes by cyber criminals.

Financial performance. Healthcare organizations might achieve efficiencies and lower employee and process costs due to the implementation of AI and other technologies. However, weighing the cost of AI or new technology against its benefits can present dilemmas at a time when much of the industry is experiencing financial challenges.

Workforce. As the healthcare industry implements more AI and advanced technologies, how work is done and who does it will change. The tech-savvy skills required to operate in this new environment could lead to turnover of employees who lack those skills. That turnover could raise an organization's legal, reputational, and cultural risks. Organizations might need to provide education and training to prepare their workforce for the advanced technology-supported future state.

Impact on patient care and reputation

Many significant benefits of AI and new technologies relate to improved patient care from enhanced diagnostic and treatment capabilities. However, many of those same benefits can be eliminated or even reversed should the underlying data become compromised, resulting in incorrect diagnoses and ineffective treatment protocols. Additionally, there is a risk that AI models have limitations based on the data used to build them, resulting in biased clinical assumptions for certain underrepresented patient populations.

Recommended reading and source list

- Melissa D. Berry, "Understanding the Advantages and Risks of AI Usage in Healthcare," Thomson Reuters, Sept. 27, 2023.
- Shashank Bhasker, Damien Bruce, Jessica Lamb, and George Stein, "Tackling Healthcare's Biggest Burdens With Generative AI," McKinsey and Company, July 10, 2023.
- Jon Moore, "AI in Health Care: The Risks and Benefits," Medical Economics, March 15, 2023.

2. Risk area: Competition

Incumbent health systems have been competing against each other for decades and now face competition for patient business from nontraditional companies entering the healthcare delivery space. Recent market entrants include Amazon, CVS Health, Walgreens, Walmart, Best Buy, and Costco. Their growing interest in providing primary care, home health, and other health services is expected to have a big impact on the competitive landscape in healthcare.

Examples of such market penetration by nontraditional companies include:

- In 2023, Amazon acquired One Medical, a national primary care organization offering both in-office and virtual services.
- Walmart Health launched in 2019 as a one-store pilot and has grown to more than 30 sites next to or inside Walmart Supercenters. The sites target consumers with little or no health insurance who live in underserved areas. Walmart Health services include primary and urgent care; labs; X-rays and diagnostics; dental, optical, hearing, and behavioral health; and mental health counseling. Walmart recently announced its plan to expand its network to more than 75 sites in 2024 to compete with large healthcare and retail organizations building and expanding their own primary care footprints.
- CVS Health acquired Oak Street Health and the direct primary care provider's 169 sites in 2023, expanding CVS' primary care service line – especially for Medicare beneficiaries living in underserved communities. The Oak Street acquisition followed just months after CVS acquired Signify Health, a home health and technology company. The acquisitions bring two new service lines into an organization with an already large footprint in the pharmacy and health insurance space.
- Costco partnered with Sesame to provide discount pricing to Costco members on a range of outpatient medical services, including telehealth visits for $29 and online mental health therapy visits for $79.

Although many of these acquisitions and partnerships are still relatively new, the competitive landscape in primary care as well as other healthcare services is likely to change as large retail and technology companies enter the market and create new competitive risks for incumbent health systems.

Other risk areas affected

Cybersecurity and data privacy. Much of this new market vertical integration is taking place outside of the traditional healthcare market. Inexperienced retailers and consumer technology companies might bring cybersecurity and data privacy risks as they integrate with other provider organizations' disparate IT systems and applications.

Financial performance. Most new market entrants are diversifying into primary care, home care, or other ancillary healthcare services. As a result, revenue from those targeted services might take a hit at incumbent hospitals, health systems, and medical practices as the new competitors siphon off patient volume and patient revenue in coming years.

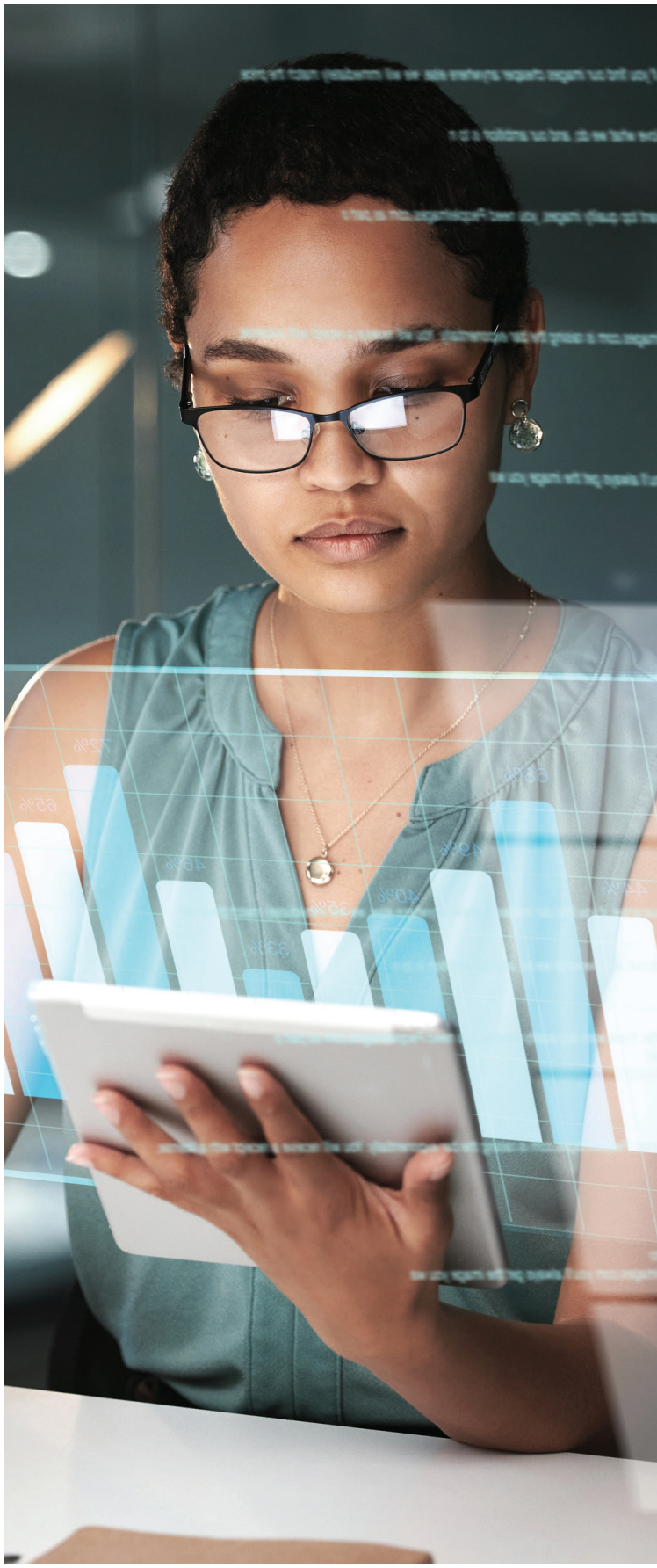
Workforce. The entry of nontraditional companies into the healthcare market might increase competition for healthcare workers who are already in short supply. This increased competition, along with the "deep pockets" of new entrants, many of which are publicly traded investor-owned companies, could raise the wage levels required to retain current staff within hospitals, health systems, and medical practices.

Impact on patient care and reputation

Although it might be too early to conclude, the entry into the primary care market by large retail and technology firms could increase the competition for primary care physicians, reduce the number of physicians employed by traditional physician practices and health systems, and potentially reduce access to primary care services for patients that currently rely on health systems and physician practices.

Recommended reading and source list

- "5 Things to Know About Amazon's Recent One Medical Acquisition," American Hospital Association, March 7, 2023.
- Rebecca Pifer, "Walmart Health Plans Clinic Expansion in 2024, Pushing Into 2 New States," Healthcare Dive, March 2, 2023.
- Heather Landi, "CVS Closes $10.6B Acquisition of Oak Street Health to Expand Primary Care Footprint," Fierce Healthcare, May 2, 2023.
- Heather Landi, "Costco Expands Healthcare Footprint, Teams Up With Sesame to Offer Members $29 Virtual Care Visits," Fierce Healthcare, Sept. 25, 2023.



3. Risk area: Cybersecurity and data privacy

The healthcare industry continues to be a top target for cybercriminals due to the sheer number of IT systems and applications healthcare organizations maintain. The systems and applications include electronic health record (EHR) systems, imaging machines, lab and pharmacy applications, scheduling applications, patient monitoring equipment, telehealth platforms, and voice over internet protocol (VoIP) phones. Healthcare is also attractive for bad actors because of the large volume of valuable PHI, increased IT connectivity between providers and vendors, and the industry's financial challenges that restrain investment in more secure technologies and cybersecurity best practices.

Cybersecurity and ransomware risks could continue to increase as healthcare organizations become more dependent on IT to run and support most of their operational, clinical, and financial processes and as IT complexity accelerates each year. These risks affect patient care, financial losses, legal and regulatory compliance, and reputation risk.

During the first six months of 2023, more than 40 million patients were affected by 327 data incidents reported to the U.S. Department of Health and Human Services Office for Civil Rights, according to Fortified Health Security's "2023 Mid-Year Horizon Report." That's a 104% increase in the number of data breaches over the same period in 2022 (160 incidents). Hacking and IT incidents were the most common type of data breach in the first half of 2023, accounting for 75% of the breaches.

Although cyberattacks and ransomware events aren't the only ways to slow or shut down clinical operations (others include employee strikes and natural disasters), cyberattacks throughout 2023 have served to highlight the importance of an organization's ability to become operational again after a

full or partial IT shutdown. Being prepared to respond to an extended IT shutdown while continuing to care for patients and communities remains one of the most significant risks facing healthcare providers.

Other risk areas affected

Financial performance. According to a study conducted by researchers at the University of Minnesota, patient volume at hospitals falls by roughly 20% during the first week of a ransomware attack. The drop in patient admittance can be attributed to an organization's lost ability to provide care through testing and images while technology systems are down or being repaired. Additional costs come from time associated with claims submitted and IT downtime recovery.

Workforce. The stress on a healthcare organization's workforce from an extended IT outage caused by a cybersecurity incident can't be understated. The workplace disruption experienced by all workers within an organization goes beyond transitioning from EHR systems to paper and pencil clinical documentation. Every workflow could be challenged, such as delayed communication of imaging and lab test results or the need for nurses to spend more time in a patient's room while monitoring systems are offline. Most workers will experience a high-stress work environment during the outage. Stress will continue after the outage as workers try to recover clinical documentation and related revenue cycle functions during the months following the incident.

Impact on patient care and reputation

A healthcare organization's ability to provide high-quality care and to continue to serve its customary volume of patients likely will diminish during a cybersecurity incident. Without immediate access to EHRs, test results, electronic patient monitoring equipment, and other information technology, caregivers are put at a potentially life-threatening disadvantage. The impact to a healthcare organization's ability to provide patient care during a cybersecurity incident can have a significant effect on its reputation in the community.

Recommended reading and source list

- Rosie Talaga, "327 Healthcare Data Breaches Reported so Far in 2023," Becker's Health IT, Aug. 10, 2023.
- "2023 Mid-Year Horizon Report," Fortified Health Security, July 2023.
- Hannah Neprash, Claire McGlave, and Sayeh Nikpay, "We Tried to Quantify How Harmful Hospital Ransomware Attacks Are for Patients. Here's What We Found," Stat, Nov. 17, 2023.

4. Risk area: Financial performance

Although inflation rates eased in 2023 compared with 2022, healthcare providers still are experiencing increased costs of medical equipment, supplies, and prescription drugs without a corresponding increase in payor reimbursement rates, leading to lower margins.

Labor-related issues such as worker shortages, labor strikes, and staff turnover also contribute to rising expenses.

Further, the cost to access capital related to new loans or refinanced debt has significantly increased over the past 18 months. The federal funds rate has increased from near 0% pre-2022 to a range of 5% to 5.5% at the end of 2023. Lower margins compounded by higher costs to borrow money make it more difficult for providers to invest in patient care capabilities, upgraded or new equipment and facilities, service line or geographic growth, cybersecurity, new technologies, and more.

Other risk areas affected

Cybersecurity and data privacy, and AI and new technologies. Because healthcare organizations are experiencing increased financial pressures, they are challenged to make necessary investments in AI and other new technologies; information security professionals to maintain IT systems and necessary security, cybersecurity infrastructure, and software; and cybersecurity assessments.

Impact on patient care and reputation

Inflationary pressures might force providers to focus more management time on cost containment rather than their patients' experiences. That could affect the quality of care they deliver to patients, which, in turn, can affect patient outcomes and satisfaction.

Recommended reading and source list

- Healthcare Inflation: What Providers Need to Know in 2023," AccessOne, May 1, 2023.

5. Risk area: Workforce

Healthcare organizations face workforce challenges including recruiting, hiring, and retaining qualified employees as the demand for healthcare services increases with the aging U.S. population and the competition for healthcare workers intensifies. Workers leaving the healthcare sector due to pandemic-related burnout and retirements have exacerbated the challenge over the past three years.

In addition, strikes in 2023 intensified workforce issues. Nurses, allied health professionals, and mental health workers cited their concerns over wages, benefits, staffing levels, patient safety, working conditions, and employee retention as reasons to walk off the job. The strikes put stress on hospitals, health systems, and medical practices and served to reset compensation at higher levels after the strikes.

"As hospitals continue to wrestle with workforce and financial challenges, the value of strong and capable leaders in healthcare has never been more important," said Deborah Bowen, president and CEO of the American College of Healthcare Executives, in a prepared statement.

That statement aside, the stress caused by the pandemic, caring for an aging population, managing fiscal challenges, and dealing with workforce issues might put hospitals, health systems, and medical practices at risk for higher turnover in the C-suite in 2024.

Other risk areas affected

Financial performance. Costs associated with travel nurses have been declining, while costs to hire and retain clinical staff and health system leadership have increased and have affected financial performance.

Impact on patient care and reputation

Labor strikes, staff shortages, and the retirement of experienced clinicians result in an increased risk to patient care as temporary and/or less experienced staff serve patients.

Recommended reading and source list

- "Study Projects Nursing Shortage Crisis Will Continue Without Concerted Action," American Hospital Association, April 13, 2023.
- Tami Luhby, "Nursing Schools Are Turning Away Thousands of Applicants During a Major Nursing Shortage. Here's Why," CNN, Oct. 5, 2023.
- Kelly Gooch, "U.S. Healthcare Workers Walk Off the Job: 27 Strikes in 2023," Becker's Hospital Review, Nov. 28, 2023.
- "Hospital CEO Turnover Rate Remains Steady," American College of Healthcare Executives, Aug. 8, 2023.
- Nina Manzanares, "Healthcare Executive Turnover Reaching All-Time Highs in 2022 – What's Next for Healthcare Organizations," Adaptive Medical Partners, 2022.
- Jeff Lagasse, "Forty Percent of Healthcare Workers Experienced Workplace Violence in the Last Two Years," Healthcare Finance, June 7, 2023.
- Kevin Holloran, Richard Park, Sarah Repucci, "Controlling Labor Costs Will Be Key to NFP Hospital Margin Improvement," Fitch Ratings, Oct. 2, 2023.

KODIAK

How can Kodiak help your organization?

Kodiak offers both proprietary technology and deep industry experience to more than 1,850 healthcare organizations to address these five top management risks for 2024 and many other risks as identified in our previous annual top risks reports.

Please contact us today to discuss how our team can use our technology, deep expertise, and experienced resources to support your organization's 2024 internal audit and compliance work plans and address these top risk areas.

Scott Gerard
Vice President, Risk and Compliance, Kodiak Solutions
+1 818 325 8457
scott.gerard@crowehrc.com

George Bezzerides
Director, Risk and Compliance, Kodiak Solutions
+1 916 266 9592
george.bezzerides@crowehrc.com

Kodiak Solutions

CHC2402-007B