Top risks for healthcare providers — 2023

Healthcare providers navigate multiple risks, cautious but empowered

pwc

Content

Emerging from the pandemic and its lingering effects, healthcare providers face a host of new and ongoing challenges. According to PwC models, the industry is undergoing a $1 trillion revenue shift away from traditional payers/providers, with new entrants disrupting traditional business models to meet changing consumer expectations. Staff turnover, burnout and vacancies are widespread. Demand for personalized services, new treatments, virtual care and removal of access barriers (transportation, language, income) continues. Patient trust is an ongoing concern.

Providers also face a range of macroeconomic and other external risks. Inflation, high labor costs and supply-chain bottlenecks are ongoing. Cyber threats are evolving and exploiting new technology and devices used on provider networks. Fraud tactics, too, are evolving in tandem. Regulatory changes continue on many policy fronts: privacy, ESG, employee safety, Medicare, Medicaid and patient billing, among others. Stakeholders — from patients and employees to communities and investors — are themselves scrutinizing provider operations and governance and exerting pressure.

As noted in our Next in health services 2023, with healthcare's shift toward digitization and customer centricity, business and operations risks are also evolving, requiring a rethinking of risk management and controls. As organizations look to transform their operations, they need to be vigilant in anticipating and managing their risks in compliance, operations, finance and technology.

Amid these daunting challenges, however, lies opportunity. With the right approach, coordination and tools, providers can mitigate these risks and emerge stronger to deliver better value to their many stakeholders.

Leverage technology and insights for resilience

With proper coordination across the three lines (operations, compliance and internal audit), armed with technology and data insights, providers can mitigate these risks and position themselves for growth and resilience. Here are some of the top risks facing providers and potential mitigating actions.

Recruiting and retention: Implement retention tactics, including expanded remote and flexible-work options, career training, education and diversity, equity and inclusion (DE&I) initiatives. Conduct audits/analytics around the employee life cycle. Learn more

Patient safety and quality of care: Upgrade patient safety systems to track near misses and adverse events, creating standardized workflows, developing checklists and capturing actionable data based on safety trends. Learn more

Cybersecurity: Perform continuous monitoring of cyber exposure for additional review and testing. Track regulatory changes to ensure compliance and leverage external insights on new threats. Learn more

Margin pressure and cost management: Implement controls against duplicate vendor payments. Invest in or optimize enterprise resource planning (ERP) solutions and data analytics. Pay increased attention to charge capture, clinical documentation completeness, denial management and payroll overpayments. Learn more

New entrants and business transformation: Inventory new entrant technologies, partnerships and contractual relationships to mitigate risk through business continuity/resilience planning. Establish innovation arms to develop apps and platforms, subject to testing and review for contractual compliance. Require more due diligence, compliance reviews and auditing of compensation and contractual arrangements to mitigate Stark law, anti-kickback and false claims violations. Learn more

Sustainability and ESG: Develop a governance structure and internal controls over sustainability programs, metrics and reporting. Learn more

Digital transformation and automation: Take an enterprise-wide approach to data governance, discovery, protection and minimization. Optimize IT infrastructure to support continued digitization across the patient population and the move to a remote or hybrid workforce. The technology platforms, applications and tools your company uses should undergo the same level of scrutiny and testing applied to network devices and users. Learn more

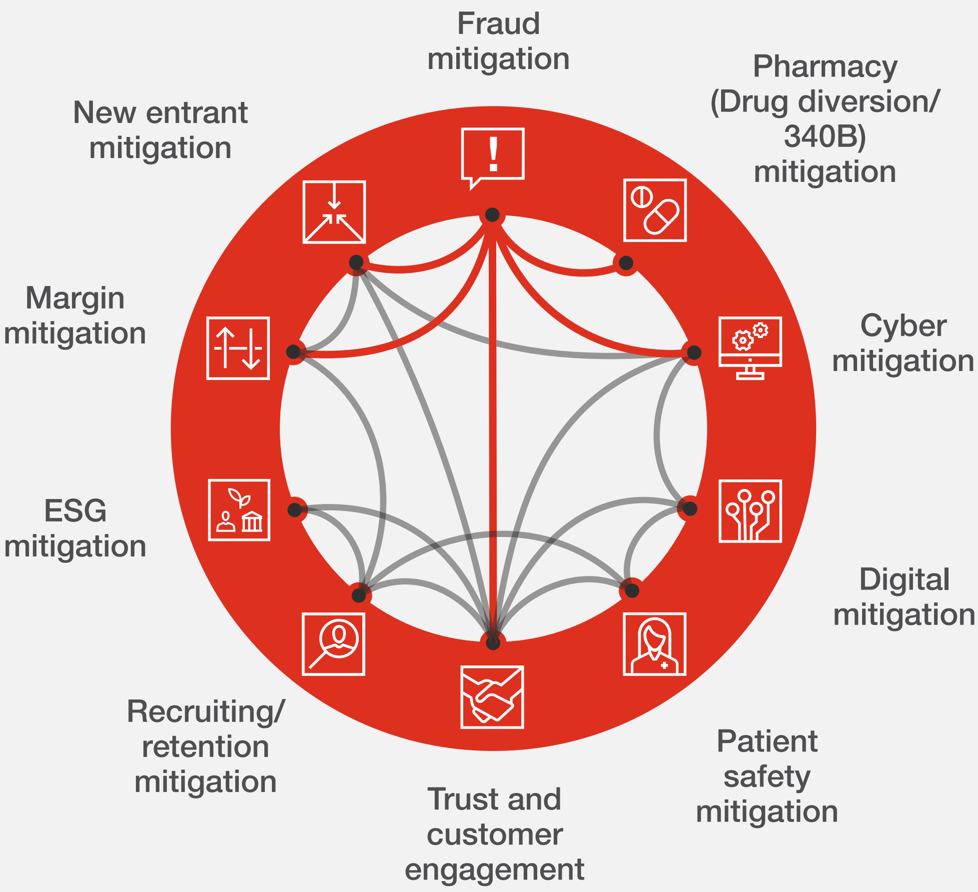
Fraud, waste and abuse: Strengthen review and monitoring to flag overpayments, denials, write-offs, claims, contractual breaches and scams. Improve monitoring of regulation updates to implement an effective regulatory change-management process. Learn more

Pharmacy: Deploy third-party analytical tools, including split-billing software and technologies, to help pharmacy departments adopt a data-driven approach to managing inventory and 340B program compliance risks better. Complement those tools with increased monitoring and auditing. Learn more

Trust and customer engagement: Take steps to improve patient access to care. Establish patient advisory boards to gather insights on patient needs and preferences. Prioritize diversity in workforce and leadership and invest in serving underserved communities. Assess and optimize patient-satisfaction monitoring processes. Learn more

The risk nexus: Where mitigation impact gets amplified

With many of these risks intersecting, mitigation actions in one area can have a compounding effect on resilience elsewhere. Mitigation of fraud risks, for example, has the potential to help you reduce risk in other areas such as cyber, margin, new entrants, pharmacy and trust. See the mitigation relationships map below.



Risk highlight
Recruiting and retention

Back to List

The healthcare industry has not escaped the Great Resignation. According to the Bureau of Labor Statistics, half a million people are quitting healthcare-related jobs each month. The paradigm around employee management and engagement also shifted dramatically during the pandemic. Organizations are now rethinking everything from compensation and benefits to taxation, regulation and workforce culture, including how to handle the shift to a hybrid/remote workforce.

Clinical workforce shortages pose risks to the healthcare industry, including significant margin losses and, in some cases, unit and even hospital closures. Many providers are bearing the cost — and risk — of temporary/per diem clinical staff. At the same time, providers are focused on fostering a diverse, equitable and inclusive workforce while putting recruitment and retention strategies at the forefront of DE&I success.

Related risks include:

- Diversity, equity and inclusion (DE&I)
- Onboarding/offboarding life cycle
- Clinical workforce recruiting; contract labor
- Remote workforce
- Talent management
- Culture

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

Management teams are working closely with human resource departments to attract talent. Some are developing strategies around the use of social media, creative team models and remote-work options to attract talent while also evaluating professional employer organizations to support out-of-state remote work. Some are mitigating the costs of temporary staffing agencies by developing their own talent pools. Meanwhile, those that have embedded retention strategies such as tenured models, career ladders and leadership development programs have felt the retention churn the least.

What new or different activities can the second line do to mitigate risk in 2023?

Second-line stakeholders have helped monitor for new remote work-related risks and risks resulting from lean staffing models, especially medical malpractice risk. Many have enhanced training and education to reduce turnover, while increased reliance on temps has helped weather the staffing shortage. We see second-line stakeholders facilitating "enterprise-wide people surveys" to understand the pain points associated with staffing and retention such as DE&I. Identifying "people's champions" from operational teams to socialize culture and implementing retention-building DE&I initiatives are also key. As part of promoting an ethical and compliance culture, the second line must also promote the importance of DE&I and work/life balance. It's up to leadership to shift the culture — set the tone from the top — while corporate compliance must continue advising on key compliance metrics around monitoring and tracking hotline inquiries to help avert undesirable trends.

What new or different activities can the third line do to mitigate risk in 2023?

Many want internal audit to assess issues around the employee life cycle, including recruitment, onboarding and offboarding, retention, performance management and payroll. DE&I-focused audits and analytics, as well as remote-work programs, have helped providers not only mitigate these risks but determine how well policies and practices had been operationalized across the organization — making sure the organization is walking the walk.

Risk highlight

Patient safety and quality of care

Back to List

Clinical staffing shortages, rising mental health challenges and increasing incidences of behavioral health patients are making it more difficult for healthcare providers to properly do their jobs. Reports of burnout are climbing, which may be putting patient safety and quality of care at risk. Indeed, a recent survey found that 31% of healthcare leaders see talent and retention as one of the top business risks.

Although virtual care is alleviating some pressure by making it easier for physicians and others to connect with patients, it's also bringing new concerns around whether medical providers can accurately diagnose and treat conditions remotely. Medical malpractice claims are stable at present, but persistent staffing shortages could result in more errors, harmful outcomes and litigation. It's up to healthcare leaders to aggressively manage burnout risks and turnover by prioritizing recruitment, retention and clinician resilience.

Related risks include:

- Staffing shortages
- Cognitive biases and diagnostic error
- Telemetry monitoring
- Patient harm, quality/safety
- Infection control
- Capacity and utilization
- Virtual care
- Continuity of care
- Employee safety
- Medical education

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

Management teams are working to standardize processes, provide better insights and empower time-strapped clinicians and staff to reduce barriers to care. Organizations are upgrading patient safety systems used to track near misses and adverse events, and they're implementing evidence-based systems and performance improvements to mitigate the risk of future events. Organizations must report incidents to ensure quality of care and remain hypervigilant about daily operations. They must also be aware of when these events occur and provide actionable data to predict and prevent repeat incidents. The focus on governance over patient safety programs and monitoring over clinical and safety protocols have increased, along with the implementation and awareness of required safety culture elements.

What new or different activities can the second line do to mitigate risk in 2023?

Second-line stakeholders have been instrumental in helping to monitor and report on patient safety incident trends while creating standardized workflows designed to streamline quality improvement projects, processes and their impact on health outcomes and quality scores. They're also creating checklists and developing actionable data based on current safety trends to further mitigate risks and provide education around patient safety protocols. Additionally, regulatory compliance and corporate compliance are supporting the review of policies, procedures and processes to ensure that activities are aligned to regulations.

What new or different activities can the third line do to mitigate risk in 2023?

Many are asking internal audit to focus on evaluating processes and controls within the infection control spaces. That includes those within central sterilization as well as on the organization's overall compliance with established patient safety programs and adverse-event reporting systems and processes. Internal audits have been used to support the walk-through of inpatient and ambulatory floors and determine if proper safety protocols are being followed. They're also used to look at departmental efficiencies — as well as reviews from a virtual care lens — to ensure that patients are scheduled for the appropriate follow-up care. Many are reviewing previous inspection reports and national and organizational safety trends to determine if remediation efforts currently impacting the organization have been sustained.

Risk highlight
Cybersecurity

Back to List

With more healthcare industry players working from home, and with malware, ransomware, phishing and other cyber threats continuing to evolve, cybersecurity concerns within the sector are growing. According to PwC's 2022 Global Risk Survey, 60% of healthcare industry leaders had planned to increase spending on managed cybersecurity services in 2022, while many reports have shown that health-related data, industry and personal, have become prime targets for cyber criminals. Further complicating matters is the industry's reliance on nontraditional devices, most of which are used on organizational networks. An attack on these devices, which hold critical — even life and death — information, can have devastating consequences. Healthcare providers must focus on safeguarding these technologies.

Related risks include:

- Cloud security
- Network security
- Data security
- Emergency preparedness and IT resiliency
- Identity and access management
- Ransomware and cyber attacks
- Breach response

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

Most IT functions already have a dedicated cybersecurity team using various technologies to enable their monitoring and response activities. Likewise, most teams watch for new or potential system vulnerabilities and look for ways to patch or otherwise mitigate issues to prevent exposure. An organization's infrastructure and safeguards will also play a key role in preventing and detecting potential threats. Most important, though, is staying current on both external insights around threats (e.g., the most recent exploits being leveraged and the current focus of cyber criminals) as well as the health of the internal ecosystem (e.g., up-front management of systems/devices brought onto the network, clear and cohesive response to threats in a timely manner).

What new or different activities can the second line do to mitigate risk in 2023?

As regulatory requirements around cybersecurity and associated exposures continue to evolve, compliance and legal teams play a critical role in helping their organization stay current and compliant. Second-line functions must interpret and apply new and changing regulations and, perhaps most critically, monitor changes as regulations move from draft to final, a slow and lengthy process. Regulatory complexities also make it difficult to correctly and effectively implement requirements, which is where a partnership between the second line and management is critical. Organizations need to work together to achieve something that is both feasible and effective.

What new or different activities can the third line do to mitigate risk in 2023?

As an independent assurance provider, internal audit can benefit many organizations by providing a second opinion on such matters as the risk landscape being considered and mitigated, the interpretation of various new and emerging regulations, and the external view and testing of the organization's prevention and detection controls. Many internal audit shops, either through internal capabilities or by coordinating with outside specialists, are tasked with running periodic attack and penetration exercises for their organization. Less common, but arguably more valuable, is the shift by some internal audit teams to ongoing, real-time monitoring of the organization's cyber exposure. This can be accomplished through tools that aggregate the existing monitoring by data management and layer on top additional risk considerations. By scoring potential exposures, teams can help focus on areas of greatest value for additional review, testing and independent validation.

Risk highlight
Margin pressure and cost management

Back to List

Margin pressures and cost increases are nothing new to the healthcare industry, but recent years have been particularly trying for providers. Rising inflation, labor costs and Medicare and Medicaid volume are driving up costs, while capped payer-rate changes and low reimbursement for behavioral health patients are hurting revenues. Fortunately, finance teams have found some success in diversifying revenue sources after suffering from COVID-19's impacts by, for example, placing greater focus on philanthropy and business development.

But providers still have their work cut out for them. According to PwC models, the industry is in the middle of a five-year, $1 trillion revenue shift away from traditional providers — as well as payers. With top line still mostly tied to patient care services, many risks persist around revenue cycle operations and performance, including managing the impacts of evolving payer requirements and coding guidelines. Payers and providers must also find their footing in the evolving healthcare ecosystems or risk losing market share to competitors. Similarly, with revenue moving away from fee-for-service to more value-based contracts, providers must cut costs to stay competitive and maintain profit margin. More than ever, providers must understand where their costs are coming from.

Related risks include:

- Liquidity and cash management
- Financing and debt management
- Philanthropy and business development
- Tax
- Financial reporting

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

Management teams are working closely with their bond rating agencies to get a better sense of how much latitude they have to weather the short-term economic storm. Budgets are getting trimmed to enforce efficiency and cost savings, while vendor contracts, usage and payments are getting the fine-tooth comb. To reduce financial leakage, leaders are looking to streamline the number of vendors they work with and to implement effective controls against duplicate vendor payments. More strategically, many are optimizing existing enterprise resource planning (ERP) solutions — or investing in new ones — to gain better insights into costs and identify areas that could be cut.

What new or different activities can the second line do to mitigate risk in 2023?

Second-line stakeholders have been less involved in margin and cost management, deferring to finance leaders for direction. As organization-wide decrees to reduce departmental budgets are mandated, second-line stakeholders will need to evaluate how they too can be more efficient, directing the conversation to greater use of data and analytics.

What new or different activities can the third line do to mitigate risk in 2023?

Many are asking internal audit to assess risks related to areas that can help drive margin relief or look for cost management opportunities. A greater focus on charge capture and clinical documentation completeness and accuracy has the potential to provide margin relief. That's especially true if services are not being adequately captured and billed for, particularly as evolving payer requirements continue to plague providers trying to keep up. The same goes for an increased focus on denial management analysis, and identifying root causes to drive up-front remediation. Additionally, attention to duplicate vendor payments, the procure-to-pay cycle and payroll overpayments are areas where management teams are leaning on internal audit to help assess controls and develop analytics to highlight risks and opportunities.

Risk highlight
New entrants and business transformation

[Back to List]

The US healthcare system is ripe for transformation, both from within and by new entrants. Persistent, structural problems — poor quality, lack of access, high costs, inequity and reduced life expectancy — along with the changing expectations of patients, payers and investors, require new approaches to the delivery of healthcare services.

The industry is seeing huge investment, innovation and new entrants from the technology, telecom and consumer sectors. Providers themselves are investing heavily to transform how they operate through advances in digital health, AI and analytics, diagnostic tools, robotics, records management and workflow automation. Many other digital health trends will accelerate to make patient care more accurate, connected and personalized.

Provider organizations should expect increasing competition from new entrants, who are disrupting the legacy model by creating a more personalized, efficient approach for patients. According to PwC's 2023 Next in health services report, health organizations will need to forge partnerships in the broader healthcare ecosystem — which includes payers, employers, tech companies, retailers, pharmaceuticals, community organizations and investors — to adapt to this changing environment.

Related risks include:

- Strategy
- Corporate development; growth plans
- Organizational structures
- Third party, vendor management

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

As providers and their patients increasingly rely on the data stored and exchanged through new technology platforms, there's increasing risk around the stability and reliability of these platforms. First-line stakeholders must inventory new entrant technologies. They also need to evaluate their relationships, including contractual relationships, to mitigate risk through business continuity and resiliency planning. We also see many healthcare provider organizations establishing innovation arms developing apps and other platforms to bridge the gaps between traditional IT environments and solutions that can increase patient access and convenience. These technology transfer arms have become revenue-generators for organizations that can set up and scale new solutions successfully.

What new or different activities can the second line do to mitigate risk in 2023?

Second-line stakeholders play an important role in ensuring that an organization's innovation arms adhere to organizational policies and practices and think through legal and data-security risks. The development, testing and implementation of new technology functionality should be reviewed to ensure that new releases observe contract terms and conditions with third parties like web and cloud service providers. The second line can mitigate intellectual property risks by establishing policies and training to ensure that rights to the innovations created at the organization stay with the organization.

What new or different activities can the third line do to mitigate risk in 2023?

Internal audit has been asked to help conduct innovation technology risk assessments and evaluate the processes used within innovation arms. Ensuring that methodologies are well documented and executed is important to the quality of a product's development and release, which impacts its success and stickiness in the market. Additionally, internal audit can help organizations conduct business-continuity and resilience planning audits to protect itself from disruption if a new entrant platform dissolves.

Risk highlight
Sustainability and ESG reporting

Back to List

Businesses are facing increasing pressure from investors and regulators to manage their sustainability risk. According to PwC's Global Investor Survey 2022, 78% of investors say that managing regulatory risks is an important factor in including sustainability in their investing decisions, second only to client demands that their portfolios have an ESG lens (82%). Final SEC rules for climate change disclosures are imminent, affecting registrants' financial statements and 10-K filings. The Joint Commission has proposed its own standards for providers.

Despite the demand for investor-grade sustainability data, few companies have a strong handle on how to respond — from clearly framing a strategy around their prioritized focus areas to building accountability throughout the business and delivering complete and accurate reporting to the capital markets. Providers are working with their internal audit departments and enterprise risk management teams to help develop their ESG materiality and risk approach.

As demand from investors and regulators accelerates, it's important for internal audit to provide risk-based and objective validation, advice and insight. Internal audit can help companies comply with ESG disclosure standards, assess ESG data collection and aggregation processes and controls, measure progress toward sustainability goals, and review sustainable product claims in reporting or advertising. Its involvement is also key as the auditors have specialized knowledge and skills needed to improve the overall quality of — and management's comfort with — key nonfinancial data.

Related risks include:

- Diversity, equity and inclusion (DE&I)
- Familiarity with ESG terminology and frameworks
- Establishing an overall approach to auditing components, metrics and qualitative disclosures
- Ability to assess materiality of ESG topics
- General pain points in establishing a program to assess ESG (who, how to audit)
- Corporate culture and behavior change
- The maturity of an organization
- The evolving regulatory and voluntary disclosure landscape
- Net-zero and nature-positive commitments
- Pressure from investors and other stakeholders
- Trust and reputation

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

Management teams are creating steering committees and governance structures around their ESG reporting, which is helping them gain insight into how their stakeholders define and accept sustainability risks. A strong multi-functional governance committee can help make sure that materiality assessments align with the company's core values and will meet the needs of customers, investors and key constituents.

Management should also focus on how data will be maintained and gathered to report on items deemed material to the company. ESG data should be controlled in a manner similar to how financial data is controlled, which is often not what happens today. And management should create reporting structures with controls and processes to help deliver complete, accurate company reports that align with the company's values and goals.

What new or different activities can the second line do to mitigate risk in 2023?

Compliance teams need a seat at the governance table. This will require gaining a detailed understanding of the systems, processes and controls that can address the ESG risks identified by management and the board. These teams should help make sure the risks identified by management align to the company's values, enterprise risk management program and key stakeholder teams. The second line should consider assisting in designing controls identified by management to manage the overall ESG process, especially data collection and reporting. The second line should also assess the controls in place to determine if they operate as intended by the first line.

What new or different activities can the third line do to mitigate risk in 2023?

As the third line, internal audit has the benefit of understanding an organization's internal controls, segregation of duties, business processes and systems. It also has experience with general risk management, including conducting enterprise risk management, monitoring corruption and auditing health and safety. This knowledge and experience makes internal audit a logical choice to provide risk-based and objective validation, advice and insight with regard to ESG. It can provide comfort over sustainability metrics by assessing design and effectiveness of internal controls over the ESG program, metrics and reporting. Internal audit can also link ESG risks to ERM risks and business objectives, and include these in the scope of future internal audits. Further, it can verify the internal controls around the data going into an organization's sustainability reports. Finally, internal audit can provide readiness assessments pending global requirements, such as the SEC's proposed disclosure rules.

Risk highlight
Digital transformation and automation

Back to List

Healthcare providers are more dependent than ever on digital advances to meet demand for new treatments, personalized services, access to care and lower costs. The HIMSS 2022 Future of Healthcare Report found that 80% of providers plan to increase investment in technology and digital solutions over the next five years. Artificial intelligence, natural language processing, robotic process automation and cloud are just some of the technologies companies are adding into their operations.

Providers must, however, make sure they're using technology not just to address margin pressure but also to improve patient outcomes and create a positive experience for employees. When used correctly, digital tools, including analytics and automation, can manage compliance risks, better protect patient and staff data, reduce healthcare costs, eliminate process inefficiencies and much more. Now's the time to assess your digital capabilities to understand the risks within your current systems and to deploy the technologies needed for success.

Related risks include:

- Cloud attacks
- Increase in operational technology attacks
- Ransomware attacks
- Inability to align staffing with demand
- Reduced patient volume due to technology inefficiencies
- Security/privacy risks of physical and electronic PHI
- Unfavorable publicly available data
- Patient harm; quality/safety

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

CISO officers are working closely with the rest of the C-suite to create a security mindset across their organizations. They're also building a foundation of data trust by taking an enterprise-wide approach to data governance, discovery, protection and minimization. Roadmaps are created from cyber risk quantification to real-time cyber risk reporting. Third-party trackers are being used to discover the weakest links in the supply chain, while software vendors are being scrutinized against expected performance standards. Any software and applications the company uses should undergo the same level of scrutiny and testing that network devices and users do.

What new or different activities can the second line do to mitigate risk in 2023?

Second-line stakeholders are bringing together advanced technology and data and expertise to create innovative products, unexpected solutions and sustained outcomes. They're also protecting value by navigating uncertainty, building trust and bolstering resilience to disruptions, change and cyber threats. Creating confidence in cybersecurity will help companies meet digital disruptions head-on and manage threats while capturing the benefits of digital transformation. The second line should also support the buildout of the governance model for AI use. By swiftly addressing changes in a rapidly evolving regulatory environment, providers can reimagine risk and unlock opportunities to drive business growth.

What new or different activities can the third line do to mitigate risk in 2023?

Internal audit is being asked to do more than uncover what happened in the past. Audit teams are now expected to offer agile, dynamic views of risk and to combine data and technology to deliver assurance and risk insights. The goal? To improve processes and risk management in the present and prevent issues in the future. Data is used to identify behavioral trends and root causes to uncover blind spots that may present an opportunity for a cyber threat. AI is providing greater risk coverage across the organization, leveraging this data driven approach and influencing the strengthening of first and second lines through digital collaboration and continuous monitoring.

Risk highlight
Fraud, waste and abuse

Back to List

Combating fraud has always been an issue for healthcare providers, but new risks continue to arise. The rescinding of pandemic waivers, additional requirements for the CURES Act, and the ongoing fraud, waste and abuse (FWA) efforts by CMS have expanded the focus of compliance departments. At the same time, new care and partnership models, among other emerging regulations, require more due diligence, compliance reviews, regulatory change management monitoring and proper implementation of regulatory and contractual arrangements. With regulations constantly changing, many organizations are concentrating their auditing on fair compensation practices and contractual arrangements to ensure fair market value and to mitigate physician self-referral (Stark law), anti-kickback and false claims risks.

Fraud itself is evolving, fueled by new tools and digital access to systems and data. Legacy FWA controls, effective in their time, are no match for today's tech-savvy bad actors.

Related risks include:

- Coding and billing compliance
- Physician compensation analysis
- Provider privileging and credentialing
- Price transparency rule
- No Surprises Act
- Advanced practice provider (scope of practice)
- Coronavirus Aid, Relief, and Economic Security Act (CARES Act) provider relief funds and federal grant compliance

Risk management:

> **What new or different activities can the first line do to mitigate risk in 2023?**

Management within revenue-cycle teams should develop key performance indicators to monitor usages of services and leverage technology to quickly flag claims or contractual arrangements outside the established thresholds. Finance should continuously monitor levels of overpayments, write-offs and significant increases with specific service lines to identify early warning signs of FWA.

> **What new or different activities can the second line do to mitigate risk in 2023?**

Compliance can proactively monitor new and updated regulations, while also facilitating the regulatory change-management process. In some cases, compliance will confirm and audit how business teams implement new policies or processes to help them conform to regulatory changes. Compliance should also leverage their risk assessment processes to identify more risk-based audits that can be done alongside any operations and internal audit. Monitoring KRIs can also help identify risk areas based on internal and external data sets.

> **What new or different activities can the third line do to mitigate risk in 2023?**

Internal audit should review any updated processes resulting from a regulation change. An independent review of controls and procedures will instill confidence that processes are working as intended. A review of overpayments, denials and write-off trending analysis from internal processes and external government audits can help to account for and reflect those dollars in subsequent reporting.

Risk highlight
Pharmacy

Back to List

Pharmacy departments across the country have been navigating a tumultuous risk environment for quite some time. Their continued focus on inventory and waste management has been complicated by persistent national supply shortages and by widespread stockpiling of critical pharmacy items. Moreover, the 340B drug pricing program, which offers substantial discounts to eligible healthcare providers and covered entities (e.g., disproportionate share hospitals, critical access hospitals and sole community hospitals), faces increased regulatory scrutiny — potentially jeopardizing a key profit-generating segment of many provider organizations. Monitoring risks related to inventory management, drug diversion and 340B compliance will be a critical focus of risk management teams going forward.

Related risks include:

- Drug diversion
- 340B compliance
- Pharmacy inventory management
- Speciality pharmacy operations
- Opioid prescribing pattern

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

Healthcare providers typically have committees that provide governance and oversight over drug diversion and 340B programs. These committees often consist of cross-functional stakeholders spanning the pharmacy, clinical operations, finance and IT departments who are responsible for developing policies and procedures — including self-monitoring and audit strategies — to minimize the risk of drug diversion and to maintain 340B program integrity. Stakeholders are constantly evaluating third-party analytical tools, including split-billing software and technologies, that help pharmacy departments adopt a data-driven approach to managing inventory and 340B program compliance risks more effectively and efficiently.

What new or different activities can the second line do to mitigate risk in 2023?

Second-line stakeholders responsible for maintaining drug diversion and 340B program integrity typically perform monthly manual self-audits using a random sampling approach, testing between 30 and 50 samples, to identify potential drug diversion or 340B noncompliance. However, given the heightened risks in pharmacy departments, these teams are increasingly adopting data analytics and technology to support their monthly monitoring activities, integrate data from disparate systems, automate testing and provide ongoing reporting. A tech-enabled audit/monitoring approach helps second-line teams:

- Automate monitoring of full population of transactions
- Facilitate a targeted sampling approach in lieu of random sampling
- Monitor 340B programs for cost saving opportunities on a transactional basis
- Empower stakeholders with data-driven insights to remediate issues and optimize resources
- Harness the value of data to support decision-making across the organization

What new or different activities can the third line do to mitigate risk in 2023?

With the exponential growth and mounting complexity related to drug diversion and 340B programs, providers are increasingly working with internal audit departments to include audits related to inventory management, drug diversion and 340B in the organization's risk assessment and annual audit plans. To satisfy the Health Resources Services Administration's annual audit expectation, many providers lean on external vendors to perform annual 340B assessments. Additionally, many organizations are working to embed a data analytic strategy and implement ongoing monitoring solutions as a leading practice to assess drug diversion and 340B transaction classifications. They're using split-billing software vendors to manage 340B compliance risks and increase cost savings afforded by 340B.

Back to List

Risk highlight
Trust and customer engagement

Healthcare providers are uniquely dependent on the trust of their patients. Research has shown that patients who trust their provider are more likely to seek out medical care, get essential vaccinations, make time for necessary screenings and break bad habits to live healthier lives. Unfortunately, PwC's 2022 Consumer Intelligence Series Survey on Trust found that 24% of consumers trust healthcare sector companies less than they did a year ago.

With the industry moving toward value-based care — where providers are reimbursed for the quality of care they offer — trust is becoming a larger determinant of organizational success. To increase that trust, providers must make the healthcare experience more convenient and engaging to patients. Transportation, language, online access and income barriers all need attention. Any impediments to access should be removed. Communicating how providers guard patient privacy and data will also go a long way to building trust, especially as more medical services go digital.

Data governance to protect patient privacy is particularly critical in the context of partnerships and access to novel health data streams, which are no longer limited to electronic medical records and claims. Beyond protecting sensitive health information, providers can also avoid collecting or identifying it in the first place. Techniques used in other industries, such as synthetic data creation, can be used to personalize experiences without jeopardizing patient information. Meanwhile, cryptography and decentralization offer future opportunities for patients to give providers visibility into a broader array of health data streams while maintaining control over their own health data.

Related risks include:

- Drug diversion
- Patient attrition and lack of engagement
- Digital access
- Diversity, equity and inclusion (DE&I)
- Privacy
- Culture

Risk management:

What new or different activities can the first line do to mitigate risk in 2023?

Providers must actively overcome the distrust that arises from historical disparities in care and upstream inequalities by transparently making cultural and systemic changes to their operations. First-line stakeholders are listening to and understanding patient wants and needs — often using human-centered design approaches and patient advisory boards. They're also using data analysis around patient personal values, utilization patterns and social risk factors to ensure better experiences and equitable outcomes. Additionally, first-line stakeholders are taking a hard look at the way they operate to make sure their organization reflects the communities they serve. This means prioritizing diversity in the provider workforce, especially in typically underrepresented specialties as well as creating diverse executive leadership teams and boards.

What new or different activities can the second line do to mitigate risk in 2023?

Second-line stakeholders play a critical role in building and maintaining trust. Compliance, for instance, has for many years ensured their organizations have the right tone-at-the-top messaging, linking their organization's goals and strategic objectives to ethical and equitable behaviors. Second-line stakeholders have also been working toward creating more diverse board membership, as well as managing conflicts of interest that could undermine their organization's reputation and its efforts to build trust. Finally, second-line leaders have been focused on patient data protection and privacy through information security efforts. Implementing policies, education, training and enforcement of these standards remains at the forefront of their agendas.

What new or different activities can the third line do to mitigate risk in 2023?

Internal audit may have a role to play in the near term by performing reviews over segments that contribute to building trust. Internal audit teams can assess the effectiveness of compliance programs, evaluate management's DE&I programs and support the identification of gaps through analytics. They can also help assess data protection and privacy controls by disclosing potential conflicts, data sharing and other risks, and to assess patient-satisfaction monitoring processes to determine the processes needed to garner feedback and put it into action.

A coordinated approach to risk management

How can your three lines collaborate better to mitigate these threats? Start by adopting a strategic, principles-based approach to risk management. That means establishing common standards (e.g., risk taxonomy, risk appetite and tolerances, risk assessment methodology, testing and monitoring approach, governance and oversight) and a single, integrated data model that supports those standards.

Without common standards that allow for better coordination across the three lines and across risk functions, providers struggle to align, plan and execute mitigation activities. Instead of strategic, enterprise-wide risk management, you end up with reactive risk management silos often working at cross purposes. The result can include misalignment, conflicting assessments, gaps, duplication of effort, higher costs and unreliable data.

Assess your current situation. Examine your current risk management programs to determine if they have evolved in a way that supports a coordinated, principles-based approach across the three lines.

- Do all lines participate in organization-wide strategy discussions, and do they include both value protection as well as value-creation projects in their annual plans?
- Are roles and responsibilities clearly defined within each line and across all three?
- Is there coordination regarding the perception of risk (common risk taxonomy and assessment of organization-wide risks), focus areas, scope and approach?

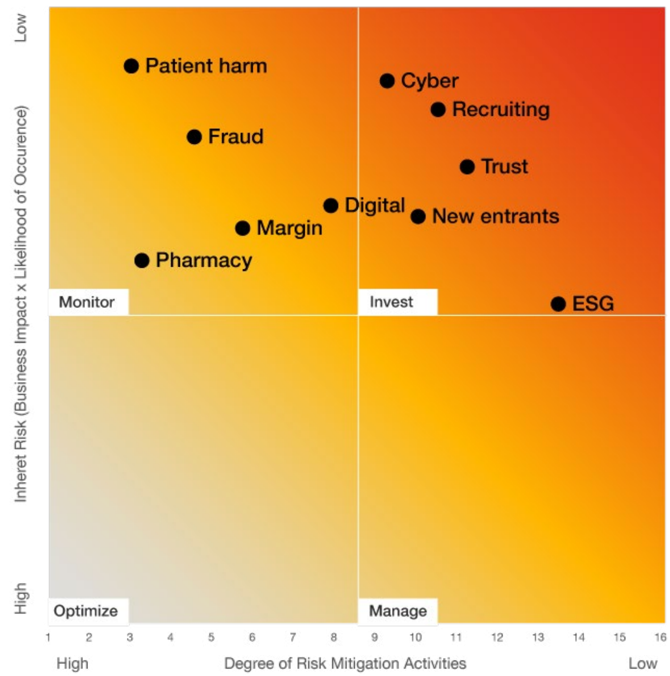
A well-coordinated, principles-based approach allows senior management to put their organization's strategy and performance at the core of their risk management programs. While many providers have components to achieve principles-based risk management in place, it's likely worth reassessing across all lines to identify where additional opportunities exist.

Identify, prioritize coordination opportunities. Once you have a principles-based approach in place, develop a plan for optimizing how the three lines can support each other's contributions. If, for example, there's a need for management to update its first-line controls, the second line (regulatory and corporate compliance) should step in to ensure that those controls conform to regulatory changes. Once the updated controls are operational, internal audit should conduct an independent review to assess their effectiveness in practice.

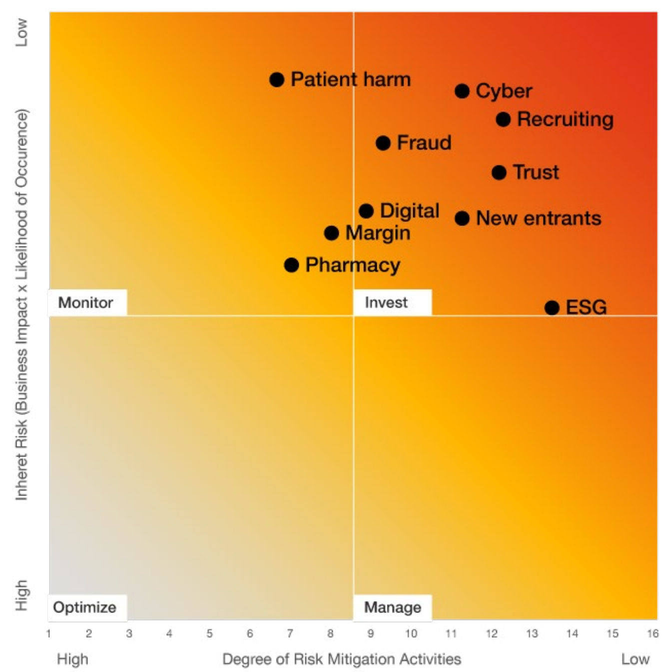
A high-level assessment of your organization's readiness to manage its top risks can help to prioritize your actions. Take a look at these scenario illustrations to see a hypothetical example of this risk mapping. The vertical axis represents the inherent risk level of each threat, the horizontal axis an organization's current ability to mitigate those risks.

Depending on where the risk falls, the appropriate response will vary. Mature risk management programs may call for monitoring (upper left quadrant), in the case of more inherently dangerous risks, or optimizing (lower left quadrant), in the case of less inherently dangerous risks. Less-developed risk programs, by contrast, may call for investing (upper right quadrant), in the case of more inherently dangerous risks, or managing (lower right quadrant), in the case of less inherently dangerous or likely risks.

Scenario 1:
Mature organization with well-developed risk management program



Scenario 2:
Newer organization with less-developed risk management program



Illustrative examples of risk management preparedness from PwC

Contacts

Tiffany Gallagher
Principal, Health Industries, Cyber, Risk & Regulatory Leader, PwC US
tiffany-anne.gallagher@pwc.com

David Merriam
Partner, Health Services, Cyber, Risk & Regulatory Sector Leader, PwC US
david.r.merriam@pwc.com

Audra Hulme
Director, Health Industries, Cyber, Risk & Regulatory, PwC US
audra.hulme@pwc.com