Top management risks in healthcare for 2022

By Scott C. Gerard, CPA;
Julia G. Breaux, CISSP, CISA, CIA;
and Andrei de Vore, CPA

Healthcare organizations continually face difficult decisions about where to allocate financial capital and human resources to mitigate undue risk exposure and enhance their return on risk.

To manage an environment of increasing risks and limited resources, healthcare internal audit and compliance departments must align their risk assessments and resulting work plans to the areas most vital to achieving their strategic goals and business objectives and maintaining compliance with critical regulatory and other requirements. This risk-based approach focuses on the areas of highest risk and suggests that less effort, if any, be applied to 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 achieved for an organization's internal audit and compliance investment.

Crowe has identified the top management risks facing healthcare organizations in 2022 using input from:

- Executive management and board members at some of the largest health systems in the U.S.
- Crowe risk assessments conducted at hundreds of health systems, hospitals, and other healthcare provider clients during 2021

The healthcare industry is challenged by unprecedented shortages within the clinical and nonclinical workforce, a rapidly changing technology environment driven by digital transformation priorities, expansion of physician organizations, and the formation of complex partnerships and vendor relationships at an accelerated pace. Because of these complexities, what might be a critical risk at one healthcare organization might not be a top risk or even relevant at another. Therefore, the following risks are being presented without a ranking, and leaders are encouraged to assess each risk and align their annual work plans to their organization's goals and objectives.

Clinical risks

Patient safety

With a rise in patient harm[1] throughout healthcare facilities, providing patient care in a safe environment should be a high priority for all clinicians and healthcare leadership. Risks include noncompliance with regulatory and industry guidelines and evidence-based practices for patient safety including environment of care, infection control, and safe handling and movement of patients. Noncompliance might result in patient harm, decreased quality scores, and decreased reimbursement.

Audits for consideration:

- Surgical safety and surgical suite disinfection
- Device sterilization and disinfection
- Hospital-acquired conditions, including but not limited to hospital-acquired infections, falls, and pressure injuries

Behavioral health

Due to the heightened focus on social issues throughout the nation and an increase in mental health issues brought on by the COVID-19 pandemic, the importance of behavioral health has reached an all-time high. Risks include missed or incomplete suicide risk screening and mental health assessment, unsafe environment that is not ligature-resistant, and untimely access or limited availability to services. The absence of standardized policies, procedures, and physician coverage could result in patient and staff harm and delayed or inappropriate care delivery.

Audits for consideration:

- Environmental and ligature risk assessment
- Mental health assessment and suicide risk screening
- Access to mental health services

Case management and utilization management

With greater focus on care coordination during a time of staff turnover, the case management process is experiencing greater challenges that have quality-of-care and financial implications. Risks include noncompliance with Medicare conditions of participation (CoP) (for example, patient rights such as patient choice and Medicare Outpatient Observation Notice), incorrect admission status, inadequate discharge planning, and weak transitions of care, all of which could affect quality and patient safety, leading to extended length of stay or avoidable readmission.

Audits for consideration:

- Compliance with Medicare CoPs
- Status assignment (inpatient versus observation)
- Discharge planning and transitions of care

Financial and operational risks

Workforce and executive retirements and succession planning

The increase in clinical and nonclinical worker turnover and in workers exiting the healthcare industry (due to COVID-19 burnout, statewide mandates, accelerated retirements, and more) has created many challenges and added to organizational risk. Such risk could drive higher costs (for recruiting, retention incentive programs, and use of travel nurse programs to shore up clinical resources) and adversely affect clinical outcomes through decreased quality of care due to provider shortages or use of travel nurses who are less familiar with organizational quality of care and clinical documentation standards. These challenges also might affect a healthcare organization's ability to fill openings in the executive ranks, especially in organizations where the approach to succession planning has not been formalized or well established.

Audits for consideration:

- Recruiting and retention effectiveness
- Critical department staffing levels
- Succession planning

Staff safety and security

Rising levels of opioid addiction, untreated mental health issues, and higher wait times at emergency departments have contributed to aggressive behavior toward hospital staff by patients and visitors. Risks include mental or physical harm to workers, financial losses due to workers' compensation claims and potential litigation, increased overtime and use of temporary staff, declining staff morale, and increased difficulty in recruiting and retaining staff.

Additionally, due to supply chain shortages, personal protective equipment (PPE) might not meet safety standards and might be used incorrectly, placing workers at risk for exposure.

Audits for consideration:

- Staff protection – PPE safety and environmental safety
- Workplace violence and management of aggressive behavior
- Physical security

Vendor management

In order for a healthcare organization to achieve its business goals and objectives, it must have strong contracting and oversight processes related to significant third-party relationships and vendor compliance with regulatory requirements. When a key vendor is unable to provide goods and services, the impact can be significant to the care provided by the healthcare organization.

Other significant vendor management risks include operational disruption due to lack of downtime procedures if key vendors are shut down. During a shutdown, reputational repercussions, financial losses, and patient safety are at stake regardless of whether the shutdown is caused by a cybersecurity attack (such as ransomware), a natural disaster, or a shortage of critical equipment due to supply chain interruption. A vendor's weak information system controls also can result in privacy or security breaches, and unsecured medical devices can lead to adverse service or business impacts.

Audits for consideration:

- Business continuity
- Vendor selection, management, and monitoring
- Vendor IT security assessment

Revenue cycle

With the recent pandemic, as healthcare organizations face lost revenues due to delayed surgeries and higher employment and supply costs, the ability to bill and collect for all services provided has become even more important. Revenue cycle risks include loss of reimbursement, impaired cash flow, and higher operational costs. In addition, compliance risks might come from poor patient access processes; failure to produce patient bills that are accurate, complete, and meet payer requirements; challenges in maintaining an updated and accurate charge description master; poor provider documentation; misunderstanding of government coding requirements; and lack of a well-designed and well-executed denials management process.

These challenges might be magnified for organizations that rely on third-party vendors to provide some or all of their revenue cycle functions on an outsourced basis and therefore have less day-to-day oversight and control. Additionally, risks can relate to healthcare organizations relying on automated claims billing systems for which they have limited visibility to or control over functionality. In addition, commercial payers might aggressively negotiate reimbursement terms or deny reimbursements in markets with little payer competition or where healthcare organizations wield minimal buying power.

Audits for consideration:

- Revenue cycle process effectiveness
- Clinical documentation improvement
- Expected reimbursement

Joint venture (JV) management and oversight

Within the healthcare industry, JVs are used in a variety of areas including ambulatory surgery, durable medical equipment, home health services, physician specialties, imaging centers, and urgent care centers. Healthcare organizations can have varying degrees of oversight for the JVs they participate in, and the level of oversight often is commensurate with the amount of equity invested. For larger JVs, senior healthcare system leadership might be assigned to participate in periodic board meetings; for smaller JVs, a less senior member of management might have this responsibility. Independent assessment of a JV's operational, compliance, IT, and financial risks by internal audit and compliance departments often is limited, and specific reporting of these risks to a health system's board is rare. Lack of adequate oversight and monitoring processes related to JVs can increase a healthcare organization's legal, compliance, reputational, and financial risks.

Audits for consideration:

- JV compliance program effectiveness (if JV receives funds from any federally funded program)
- JV contract compliance
- JV management and oversight processes assessment

Legal and regulatory compliance risks

Pharmaceuticals

Health systems continue to help patients who are in the grip of a full-fledged opioid epidemic, which is often overlooked amid the COVID-19 pandemic. The delay of surgical procedures because of the pandemic has led to longer opioid treatment to manage pain. In addition, an increase in depression, financial difficulties, and workplace stressors resulting from dealing with COVID-19 has led some patients and health system staff to opioid addiction (including drug diversion). Furthermore, rapidly escalating costs within the pharmaceutical supply chain have combined with new limitations implemented by drug manufacturers on the use of the federal 340B Drug Pricing Program. In addition, lack of compliance with 340B Program regulations might result in manufacturer repayments or removal from the program.

Audits for consideration:

- 340B Program compliance assessment
- Opioid prescribing analysis and monitoring assessment
- Drug diversion

Physician financial transactions

The Association of American Medical Colleges projects a shortage of 122,000 physicians across the United States over the next 10 years.[2] As a result, health systems are entering into relationships with physicians to ensure long-term medical continuity for the populations they care for. In other cases, contracts with physicians are being revised to include quality and safety components, reflecting an increased shift from fee-for-service models of care to value-based contracts.

Risks include violating federal fraud and abuse statutes (such as Stark Law and false claims and anti-kickback statutes) through payments to physicians without a contract, in excess of contractual amounts, or above fair market value. Other risks include physicians using hospital space without appropriate lease agreements with or compensation to the health system, recruitment arrangements that do not meet regulatory requirements, and failure to monitor contract and recruitment arrangement terms.

Audits for consideration:

- Physician payments
- Physician contract compliance

Emergency Medical Treatment and Labor Act (EMTALA)

EMTALA regulations require emergency departments to provide a timely medical screening exam prior to obtaining financial responsibility information. However, due to significant staff turnover, new employees might not be aware of the EMTALA and its requirements. Additionally, emergency departments must maintain EMTALA compliance when transferring a patient with an emergent condition to another facility. Noncompliance can result in patient harm, legal and reputational damages, and financial penalties.

Audits for consideration:

- Compliance with EMTALA guidelines within the emergency department
- Compliance with EMTALA guidelines for patients presenting outside the emergency department
- EMTALA transfer and receiving processes (anti-dumping)

Advanced practice providers (APPs)

The use of APPs likely will increase given a physician shortage that is only expected to worsen in coming years. It is critical for an APP to comply with scope-of-practice and supervision (if applicable) requirements established by facility or medical group bylaws and state-specific regulations. Risks include noncompliance with government regulations and payer contract requirements related to clinical documentation and billing (for example, incident-to services, split-shared visits, and modifiers) for services performed by both the APP and the physician.

Audits for consideration:

- Scope-of-practice alignment with state-specific practice authority
- Compliance with supervision requirements
- APP services documentation and billing compliance

Acute care at home

Patients admitted into the Centers for Medicare & Medicaid Services (CMS) Acute Hospital Care at Home program might not meet qualifications for an acute care at home setting. Risks include treatment delivered to patients at home that does not meet standards of care and might affect care quality and patient safety. Hospitals might not be able to fulfill staffing and technology requirements, which can affect patient experience and quality of care. Documentation and billing of services performed might not comply with government and payer requirements.

Audits for consideration:

- Acute Hospital Care at Home program admission and qualification process
- Acute Hospital Care at Home program oversight for standards of care, quality, and patient safety and experience
- Acute Hospital Care at Home documentation and billing

Technology risks

Cybersecurity and ransomware preparedness

Lack of mature controls governing cybersecurity continues to be a top risk. In recent years, the likelihood of an attack causing extended downtime for a healthcare organization has grown at an accelerated rate. While layered technology and the information security department form the digital front line to these threats, the risk impact spans across the entire organization. Risks include IT downtime throughout an organization, causing an inability to provide patient care and conduct business operations; employees falling victim to social engineering tactics; an inability to quickly recover from a substantial IT threat; attacks originating from third parties (for example, trusted vendors or providers of software patches); and unauthorized access to systems and data.

Audits for consideration:

- Ransomware preparedness and response
- Cybersecurity risk assessment
- Business continuity management

Data governance

Data governance is concerned with four basic properties for an organization: Where does the data reside? What data is leaving the organization? What data is coming into the organization? How critical is the data (for example, protected health versus personal information)? For many organizations, data governance risk lies in an inability to know the precise answers to any of these questions or to appropriately manage the data governance program. Common risk areas include the vast amount of patient data potentially residing on personal devices, unmanaged network shares, clinical devices, and myriad third-party sites.

Audits for consideration:

- Data governance program
- Third-party risk management
- Cybersecurity assessment

Biomedical devices

While biomedical devices have been used in the healthcare industry for quite some time, many organizations still do not have mature governance over biomedical device procurement, vendor oversight, and device risk management. Risks relate to a lack of layered security controls for biomedical devices – including logical access and passwords – and network segmentation. These risks can present challenges to patient safety, network security, and the organization's financial and reputational position.

Audits for consideration:

- Biomedical device governance and procurement
- Biomedical device security
- Biomedical device maintenance and third-party service-level agreement compliance

Emerging risks

Telemedicine

With a significant increase in telemedicine use, risks have increased related to noncompliance with government and payer requirements for documentation and billing of telehealth services (for example, modifiers, place of service, and consents), resulting in denied claims and lost reimbursement. Telemedicine risks also relate to technology failures or cyberattacks on telemedicine technology, resulting in system failure or disruption that can affect quality of care, patient experience, and HIPAA compliance.

Audits for consideration:

- Compliance with documentation and billing requirements for telehealth services
- IT assessment of telehealth platform and devices
- Cybersecurity assessment of network and unified communications supporting telehealth

ESG and DE&I

Organizations are facing increased pressures from key stakeholders, including their boards, executive management, employees, and consumers, to measure, evaluate, and accurately disclose efforts toward environmental, social, and governance (ESG) standards for operations, which include diversity, equity, and inclusion (DE&I). Aligning these initiatives with the organization's strategic goals and objectives presents internal and external risks.

With current market shifts, stakeholders (such as employees, vendors, and patients) want to be associated with organizations that can demonstrate their ESG focus (on, for example, climate change, pollution, energy, and natural resource consumption) through actions and reporting. Healthcare organizations can experience increased reputational risk if patients and communities feel underrepresented and misunderstood, resulting in decreased quality of care and a widening of healthcare disparities. Additionally, healthcare providers can be viewed as failing to offer services that meet the unique social, cultural, and linguistic needs of patients and communities.

Internal risks include failing to protect worker health and safety and embodying a workplace culture that lacks focus on environmental issues, governance matters, and inclusivity. Additional risks include failing to attract and retain talent, lacking trust from employees, and missing out on emerging opportunities and areas for innovation.

Audits for consideration:

- Assessment of current ESG and DE&I programs (determination of social and financial materiality, goal and metric setting, quantification and reporting of metrics and results, and board oversight)
- Executive and employee pay analysis

New regulations

Regulators are introducing legislation focused on consumer protections. These new regulations affect healthcare organizations in the areas of revenue cycle billing, patient and employee safety, and data privacy and protection. Development and implementation of processes and controls to mitigate the financial, operational, regulatory, and reputational risks associated with noncompliance with these regulations might be affected by the workforce turnover issues healthcare organizations are facing. Internal audit and compliance professionals need to understand the impact of these risks and related controls to limit exposure to the organization.

***No Surprises Act* compliance.** Risks include civil monetary penalties for each violation where a patient receives a surprise medical bill as well as reputational risks resulting in lost revenue for facilities and providers.

Audits for consideration:

- *No Surprises Act* process effectiveness
- *No Surprises Act* compliance

Price transparency. Risks include noncompliance with federal and state transparency regulations resulting in monetary fines, reputational risk stemming from public criticism if a hospital knowingly does not comply with requirements, and revenue cycle bills not matching charges posted on a hospital's website.

Audits for consideration:

- Compliance with CMS and state regulations
- Assessment of pricing accuracy

CMS vaccine mandate. Risks include noncompliance with regulations resulting in civil monetary penalties to the facility, denial of payment, and – as a final measure – termination from the Medicare and Medicaid program.

Audits for consideration:

- Vaccine process assessment
- Regulatory audit preparedness

***Coronavirus Aid, Relief, and Economic Security Act* (CARES Act) provider relief funds and federal grant compliance**. Risks include recoupment of pandemic-related funds due to inadequate support of healthcare-related expenses or lost revenue calculations and noncompliance with terms and conditions for use of the funds.

Audits for consideration:

- Assessment of pandemic reporting
- Special project: Preparation of pandemic fund submission(s)
- Office of Inspector General audit preparedness

State-regulated data privacy. Risks include noncompliance with emerging state-specific privacy regulations and reputational risk stemming from how consumers' personal data is being used and organizations' failures to fully deidentify personal information.

Audits for consideration:

- Data governance assessment
- Data privacy compliance

Physician practice clinical operations

Clinical, legal, regulatory, reputational, medical malpractice, and patient safety risks increase when key processes within a physician practice (for example, results management, referral management, medication reconciliations, device sterilization, and medication storage) are not functioning as designed.

Although the risks within a physician practice or other ambulatory site have been known for years, a few trends have caused these risks to increase in recent years. First, many health systems continue to acquire more and more physician practices, and the pre-acquisition due diligence often is focused on financial matters such as revenues, collections, and productivity instead of on clinical processes. Also, due to the volume of staff turnover within physician practices and the increase in resignations experienced across the healthcare industry, some clinical processes that were once properly functioning as designed are now not working as employees with years of process knowledge and experience leave.

Audits for consideration:

- Physician practice (or ambulatory site) clinical assessment
- Physician practice results management assessment
- Ambulatory site device disinfection assessment

Robotic process automation (RPA)

As healthcare organizations implement robotic applications ("bots") within standardized and rules-based processes (such as billing, collection, cash application, and prior authorization within the revenue cycle management process), it is critical that leadership and board members understand how these technology solutions are controlled. To provide assurance related to RPA, internal audit and compliance professionals need to understand the risks and related controls associated with the accuracy and completeness of data processed by bots, data governance processes, and access controls to prevent unauthorized and untested changes to the RPA programming (scripts and coding).

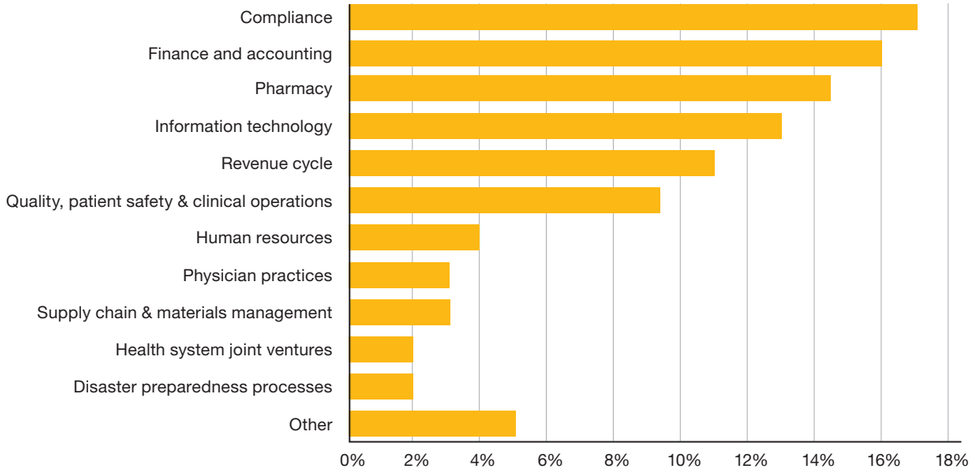
Audits for consideration:

- Review of overall RPA governance process
- Assessment of RPA security controls and disaster recovery
- Assessment of RPA change management

How audit plans compare

To help healthcare internal audit and compliance leadership prepare for risk assessment meetings and discuss with governance how their annual work plans compare to others across the industry, Crowe analyzed audit projects conducted during 2021 by the hundreds of professionals in the Crowe Audivate® user community, noting the following findings:

Audit coverage by risk area



- **Compliance** – 17% of total audits. Only a limited number of APP compliance audits were conducted during 2021, highlighting this as an emerging risk for 2022. Audits conducted within this risk category related to:
  - Physician contracting
  - Physician compensation
  - Coding and billing compliance
  - Clinical documentation improvement
  - Compliance program effectiveness
- **Finance and accounting** – 16% of total audits. This risk category contained audits related primarily to:
  - Federal grants and funding, with the CARES Act representing the largest percentage of these audits
  - Accounts payable
  - Accounts receivable and accounts receivable valuation
- **Pharmacy** – 14.4% of total audits. This risk category contained audits related primarily to 340B compliance and drug diversion, with a limited number of opioid stewardship audits conducted during 2021.
- **Information technology** – 13% of total audits. These audits included:
  - Cybersecurity assessments
  - Data backup and recovery
  - System pre- and post-implementation
  - IT vendor oversight
  - User access
  - IT governance and telemedicine technology (privacy and security)
- **Revenue cycle** – 11% of total audits. This category contained audits related to:
  - Charge description master
  - Billing and claims submission
  - Denials management
  - Patient access
  - Price transparency
- **Quality, patient safety, and clinical operations** – 9.6% of total audits. This category included audits related to:
  - Infection prevention
  - Patient safety (including surgery safety and PPE)
  - Patient handoff
  - Telemedicine and behavioral health
- **Human resources** – 4% of total audits. These audits were related mostly to payroll, timekeeping, and wage and hour matters, with a limited number of audits associated with recruiting, hiring, and onboarding.
- **Physician practice** – 3% of total audits. This category included audits related to:
  - Physician office coding and billing
  - Cash handling
  - Physician credentialing
  - Charge capture
  - A limited number of physician office clinical risk management
- **Supply chain and materials management** – 3% of total audits. Audits in this risk category related to purchasing agreements and group purchasing organizations, consignment inventory, and access to PPE supplies.
- **Health system joint ventures** and **disaster preparedness processes** – each of these risk areas represented 2% of total audits.
- "Other" internal audit topics accounted for the remaining responses.

Are these risks in your plan?

In a comparison of healthcare industry audit projects conducted during 2021 to the top risks noted by healthcare boards and executive management, the following risk areas appear to be underrepresented in many audit plans:

- Advanced practice providers, including APP compliance
- Pharmaceuticals, including opioid stewardship programs
- Workforce, specifically clinical workforce recruiting, hiring, and onboarding
- Physician practice clinical operations
- Staff safety and security
- Behavioral health

Next steps for achieving return on risk

Today more than ever, healthcare organizations' resources are limited even as the number and significance of potential risks grow. Taking these steps can help organizations make sure internal audit and compliance functions are aligned with the most significant risks they face:

- Review the top risks as part of preparing for annual risk assessment interviews and the work plan development process.
- Ensure teams are using data and technology during the risk assessment and for each project in the plan to enhance the risk assessment process, increase efficiencies, and expand risk coverage.
- Once the annual work plan is developed, compare it to the top risks and the most common audit projects conducted by those within the Crowe Audivate user community. Determine whether variances are justified for the organization.
- Continually align and reallocate your limited resources to your healthcare organization's top management risks as well as the industry's top and emerging risks to deliver the greatest return on risk.

Crowe provides both proprietary technology and deep industry experience to more than 1,000 healthcare organizations to address these top risks and many others.

Please call us today to set up an appointment to discuss how Crowe can support your work plan with technology, knowledge, and resources.

Learn more

Sarah Cole
Partner
+1 314 802 2049
sarah.cole@crowehrc.com

Scott Gerard
Partner
+1 818 325 8457
scott.gerard@crowehrc.com

Eric Jolly
Partner
+1 415 230 4956
eric.jolly@crowehrc.com

Shameka Smith
Principal
+1 314 802 2026
shameka.smith@crowehrc.com

Dan Yunker
Principal
+1 312 899 1514
dan.yunker@crowe.com

Rebecca Welker
Managing Director
+1 314 802 2055
rebecca.welker@crowehrc.com

---

[1] Stan Pestotnik and Valere Lemon, "How to Use Data to Improve Quality and Patient Safety," HealthCatalyst, April 30, 2019.

[2] Ahmed H, Carmody J (July 15, 2020) On the Looming Physician Shortage and Strategic Expansion of Graduate Medical Education. Cureus 12(7): e9216. doi:10.7759/cureus.9216.

crowe.com

CHC2299-011B