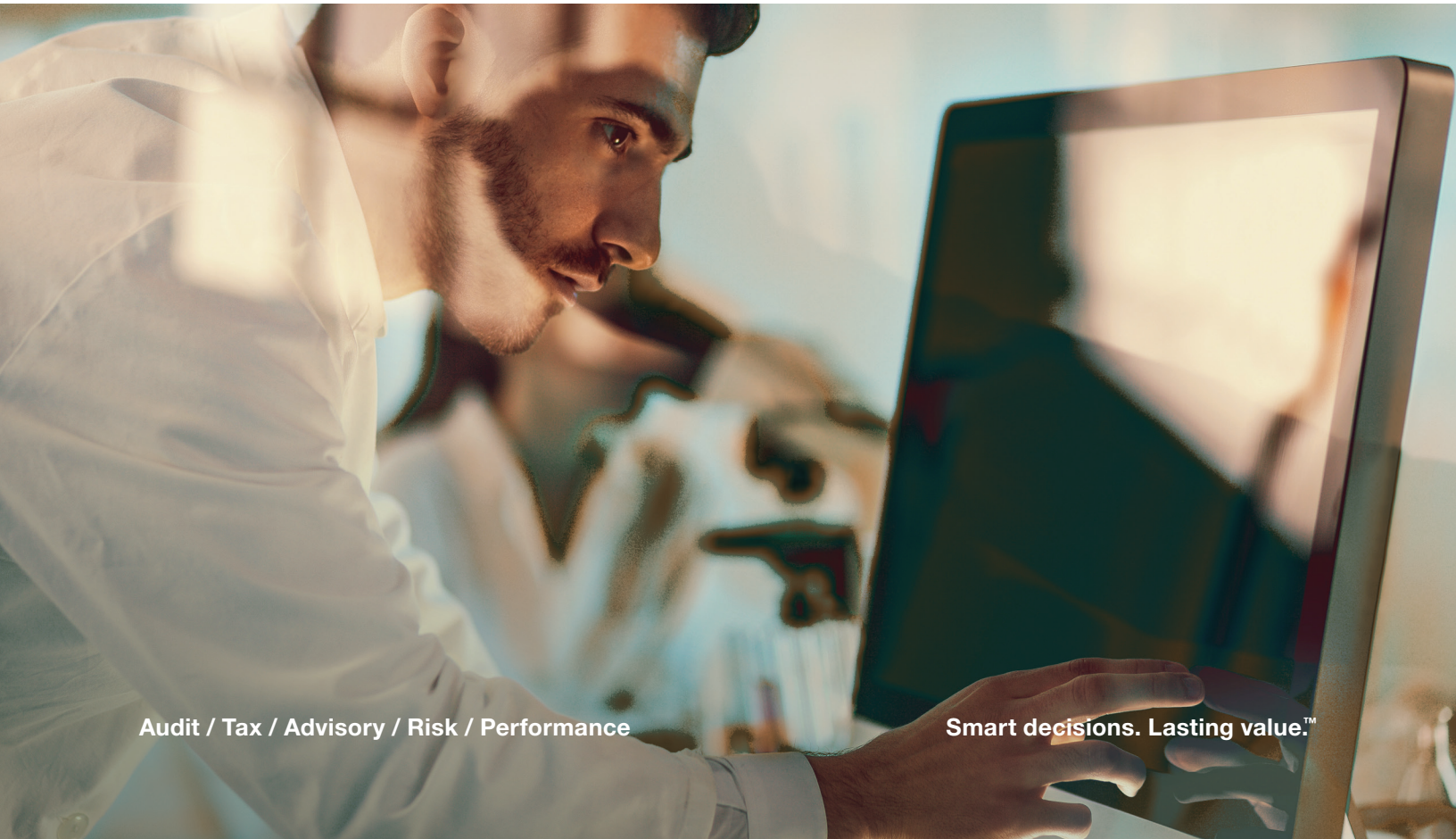
Crowe

November 2018

The Top Risk Areas for Healthcare Organizations in 2019

An article by Sarah A. Cole, CPA, and Scott C. Gerard, CPA



The growing complexity of healthcare delivery and financing is creating new risks for hospitals, health systems, physician practices, and other types of provider organizations. Each innovation – whether it's a new medical technology, a new setting of care, or a new value-based payment mechanism – brings with it unforeseen threats for which traditional internal audit and compliance programs may not be prepared.

Lack of preparation for new risks can cost a healthcare organization money and its reputation at a time when it can least afford to lose either. In a value-based reimbursement environment, every dollar is at risk. If an organization loses that dollar to a compliance problem, it can't make it up simply by adding a dollar of revenue elsewhere.

Early identification is the best strategy to mitigate those risks. To help with identification, based on what was learned in 2018, Crowe has named the top risk areas facing healthcare organizations in 2019.

Methodology

The determination of top risk areas for healthcare organizations in 2019 is based on the results of risk assessments performed in 2018 for more than 250 Crowe healthcare clients, including hospitals, health systems, physician practices, and other provider organizations.

A “risk area” is defined as anything that might impede the organization’s ability to achieve its goals in critical areas such as patient care, regulatory compliance, operations, strategic growth, and financial performance. A risk area was considered a “top risk area” based on its frequency of inclusion in client risk assessments as well as its perceived potential impact to strategic goal achievement. Twenty-three risk areas met the criteria.

What may be a top risk at one healthcare organization may not be a risk at another, so the top risk areas are not ranked. Instead, they are grouped into five categories in alphabetical order:

- Compliance
- Information technology
- Operations
- Patient care
- Revenue cycle

It is important to note that many of these top risks are multifaceted and may be relevant to more than one of the five categories.

Compliance

340B

Compliance with the 340B Drug Pricing Program remains a top concern for healthcare governance and management. Under the 340B program, eligible entities may take advantage of significant discounts in the cost of outpatient drugs, enabling them to stretch limited funds and provide more comprehensive services to low-income patients and their local communities. The 340B regulatory requirements are numerous and complex, and they often require substantial internal monitoring. Noncompliance can have significant negative financial risks ranging from regulatory penalties and manufacturer repayments to total removal from the 340B program. The numbers of audits by the Health Resources and Services Administration (HRSA) and by drug manufacturers are likely to increase again in the coming year for healthcare organizations. As a result, demand is rising for 340B program assessments and independent audits to proactively identify and resolve potential compliance concerns before an external or regulatory review.

Health Insurance Portability and Accountability Act (HIPAA)

Protected health information may be communicated or stored via paper, oral, or electronic methods. Safeguarding of protected health information in all of its forms is critical to manage regulatory, legal, reputational, and financial risks related to internal and external security threats. Failure to do so could result in civil and criminal penalties on an organizational and individual level. To minimize vulnerability to cyberattacks and privacy breaches, healthcare organizations must implement stringent controls, including risk assessments, state-of-the-art password and authentication methods, activity logging and monitoring, and "minimum necessary" access to electronic protected health information (ePHI) for IT-managed systems and for systems that are managed outside of IT (shadow IT). Healthcare organizations also must design and implement strong HIPAA privacy and security policies and processes to promote compliance and support successful completion of an Office for Civil Rights or other regulatory agency compliance audit.

The top risk areas are presented in alphabetical order first by category and then within each category. They are not ranked.

Nonphysician contracts

Healthcare systems also may face financial, legal, and compliance implications without strong controls over the execution and management of contracts for nonphysician services. Common problem areas in nonphysician contracts include the need for a single, complete, accurate, and secure database of contracts; failure to monitor contract performance and compliance against terms (resulting in legal liability and unnecessary expenses); failure to incorporate preapproved, standardized contract terms within all contracts to safeguard corporate interests; and inefficiencies in the contract negotiation and execution processes that inhibit patient care and business operations.

Pharmacy

Inadequate controls in the area of pharmacy and controlled substances can introduce significant financial, compliance, patient care, and reputational risks. Pharmacists and other healthcare providers share accountability to help prevent and detect prescription drug abuse and diversion, particularly with regard to controlled substances. To help manage the risks in this area and to support national efforts to stem the opioid epidemic, organizations must establish and enforce policies, procedures, standards of practice, and protocols in pharmaceutical prescribing, ordering, dispensing, and administration. In addition, robust inventory methodologies and routine monitoring processes are critical to help detect and address potential diversion activities.

Physician contracts and compensation

Physician contracting and compensation continue to be significant risk areas for healthcare organizations due to the complexity of contracts and compensation models and because of the regulatory risks when relationships and contracts are not carefully negotiated, reviewed, executed, and monitored. Contract review processes are vital to establish relationships and contract provisions that do not violate the Stark Law, anti-kickback laws, or other federal fraud and abuse statutes. Physician performance monitoring is also critical to identify areas where expectations and contract provisions are not being met, and careful review of compensation and bonuses is needed to reduce the potential for overpayments or underpayments and violations of federal statutes.

Information technology

Business continuity and disaster recovery

IT systems must be available and working at all times. To promote continuous availability of systems and the related data, healthcare organizations must have primary and secondary data centers for redundant operations in the event of a disaster or downtime. Each of these primary and alternative processing sites should be ready for use and must have appropriate physical, environmental, and operational controls to promote secure and continued operation when needed. Patient safety, productivity, and revenue could be severely affected if systems and data are not always available.

Cybersecurity

Cybersecurity continues to be a high priority for executive leadership, boards, and audit committees. They want to know how ePHI and other sensitive data are protected and whether system security is strong enough to withstand an internal or external attempt at unauthorized access. A robust cybersecurity program requires strong controls to prevent or minimize computer system security vulnerabilities. This includes user authentication and access controls, data loss prevention programs, network security controls, and data encryption. Also included in the cybersecurity risk area is network-connected biomedical device and internet of things (IoT) risk, which includes aspects of patient safety, HIPAA privacy, and network security risk.

IT governance

IT governance is an important component of corporate governance and is focused on delivering technology services to support business initiatives in a manner that mitigates risk. IT governance is critical to ensuring that the provision of information services is strategically aligned with the business and that adequate resources are made available to support achievement of technology and business goals. In addition, a strong IT governance program must include promoting and monitoring IT compliance with technology-oriented laws and regulations such as HIPAA, the *Health Information Technology for Economic and Clinical Health Act*, and meaningful use.

Systems access management

A well-designed systems access program and associated user provisioning processes are crucial to secure an organization's information systems and meet fiduciary and regulatory requirements. Strong controls in this area protect data and systems availability, confidentiality, and integrity by limiting access to information and resources based on the concepts of least privilege and need to know. If systems access processes are poorly designed or incorrectly implemented, ePHI and other sensitive information will be put at risk for inappropriate disclosure or manipulation, potentially resulting in fines and penalties for regulatory noncompliance and damage to the organization's brand. In addition, without strong access management controls, operating systems and business and clinical applications may be vulnerable to loss or failure due to external or internal manipulation.

The top risk areas are presented in alphabetical order first by category and then within each category. They are not ranked.

Systems implementation

The implementation of electronic health record (EHR) and other critical clinical and business systems poses a significant risk to healthcare organizations. Many operational, clinical, financial, and IT risks can result when systems are not implemented on time, within budget, and using industry standards for design, testing, training, and support.

IT risks include lack of security, poor change management, inadequate backup and recovery, improper segregation of duties, insufficient infrastructure to sustain and optimize the EHR systems after implementation, and lack of proper interfaces with other systems.

Operations

Case management

Case management, often referred to as care management, is intended to help patients reach their optimum level of wellness while promoting cost-effective, high-quality outcomes. As such, it affects both clinical and financial aspects of a healthcare organization. Absent strong controls in this area, organizations may see increased readmissions, regulatory noncompliance, and increased denials and billing problems. To minimize these risks, governance and management functions continue to seek insights into ways to optimize processes related to discharge planning, utilization management, validation of medical necessity, and patient status.

Financial performance

Business processes such as accounts payable, accounts receivable, payroll, and financial statement close are a standard part of day-to-day operations for healthcare organizations and generally are well-controlled. However, when significant changes occur in the organization or environment – such as leadership changes, regulatory changes, mergers, or acquisitions – or when new technologies supporting these processes are introduced, financial, fraud, and legal risks may increase. To minimize these risks, healthcare organizations must proactively plan for and manage change through additional process guidance as well as through increased management oversight and timely and regular monitoring processes.

Health information management

Health information management (HIM) is critical to managing compliance and coding risks. To maximize healthcare reimbursement, clinician documentation of patient encounters and services delivered must be timely, complete, and accurate. Effective HIM also is needed to support patient privacy, quality reporting, quality process improvement, and pay-for-performance decisions. EHR systems play an important role as the origination point, secure repository, and vehicle for diagnoses and care documentation. To promote accurate and complete documentation and billing, clinicians must be trained to use EHR functionality to meet documentation requirements. System access must be managed in accordance with job function, and use of copy-and-paste functionality in the EHR must be limited and managed to promote clinical documentation integrity.

Joint ventures

In the healthcare industry, joint ventures (JVs) commonly are leveraged for ambulatory surgery centers, imaging centers, radiation therapy offices, urgent care centers, and real estate investments. Collaborating with insurance payers also is on the rise as healthcare organizations seek to reduce time, cost, and regulatory burdens. JV agreements often result in complex arrangements, including the sharing of revenues and expenses between the entities. This sharing (or splitting) can be difficult to monitor if appropriate processes are not established. In addition, as there is no direct transfer of ownership, organizations typically have varying degrees of oversight for JVs. Risks related to these arrangements center around whether the parties are meeting the terms of contractual agreements and achieving performance and return on investment expectations. In addition, regulatory, IT, and compliance risks must be considered, including compliance with the Stark Law, anti-kickback laws, the *False Claims Act*, HIPAA, antitrust laws, state insurance regulations, and medical tort liability regulations. Without oversight and monitoring of operational, compliance, and IT controls in these areas, healthcare organizations may be vulnerable to fines and penalties for compliance violations and could suffer reputational and legal damages.

Physician practices

Physician integration continues to be a major area of focus as healthcare organizations work to realize the increased efficiencies and coordination required by healthcare reform. Organizations must develop processes and monitoring to effectively manage physician relationships and contracts. In addition, strong controls need to be implemented and enforced in day-to-day operations such as patient scheduling and registration, patient billing, cash handling, and prescription and medication management. Robust controls in each of these areas are critical to accomplish strategic goals in the areas of quality patient care, patient satisfaction, regulatory compliance, and revenue recognition.

The top risk areas are presented in alphabetical order first by category and then within each category. They are not ranked.

Third-party vendor management

Healthcare organizations routinely use third-party vendors in a variety of important operational, clinical, and technology capacities, usually with the intention of reaping cost savings and operational efficiencies. Third-party vendors often have access to the hospital facility and hospital data as well as direct access to patients. Risks related to use of third parties for core services must be considered carefully before contracts are signed, and they must be managed throughout the vendor relationship. These risks include failure to meet contracted performance requirements, failure to meet the financial terms of the contract, and billing for services not provided. Compliance, patient safety, and regulatory risks are also significant, and failure by third parties to comply with federal, state, and local laws can have immediate and devastating negative financial, legal, and reputational results. This is especially true with regard to weak information systems controls where vendor vulnerabilities may result in a privacy or security breach. A thorough vendor management program with ongoing monitoring of third-party entities is critical to mitigate this risk area.

Patient care

Quality and safety

Ensuring the quality and safety of patient care is inherent to the mission of healthcare providers. Diligent and continuous focus is needed to manage the countless new and evolving patient safety, quality improvement, and reporting initiatives. Healthcare organizations must balance funding and support for these initiatives with other organizational needs and goals. This is particularly difficult in light of the increasing shortage of skilled nursing staff and limited monetary resources, both of which affect quality of care and patient safety outcomes. Management is challenged to aggregate, secure, and use the influx of care data from a wide variety of EHRs, patient care technologies, and care delivery platforms. Failure to do so can have immediate and profound impacts not only on the health and well-being of patients but on the financial, regulatory, and reputational strength of the organization.

Telehealth and telemedicine

Healthcare organizations are rapidly embracing telehealth and telemedicine as a means to improve access to healthcare services, reduce or contain the cost of healthcare services, and improve the quality of services provided. In implementing the technologies and processes to support these initiatives, healthcare organizations also must implement strong controls for remote service delivery and supporting technologies. These controls are necessary to address and adhere to clinical standards (provider capabilities, credentialing, standards of care), promote high-quality care, minimize the risk of patient harm, and comply with regulatory requirements for privacy and patient data security.

Revenue cycle

Billing and collections

Management of billing and collections, including accounts receivable, is a core function required to keep revenue streams flowing to fund healthcare operations and initiatives. Healthcare organizations must produce error-free claims that are transmitted in a timely manner to clearinghouses and payers. Failure to produce bills that meet payer requirements can result in costly rework, increased denials, and lost reimbursement. To help manage these risks, many healthcare organizations have outsourced billing and collections functions. While outsourcing can help with standardization of processes, careful management and oversight of third-party provider performance are required to ensure that strategic objectives are being addressed. Risks are related to the completeness and accuracy of billing, lost revenue, inadequate denials management, and lack of visibility into controls at third-party billing and collections providers.

Charge capture

Managing the charge capture process and maintaining a complete and accurate charge description master (CDM) are essential but complex processes for most healthcare organizations. EHRs and other patient care subsystems are the genesis for charge records, which then interface with hospital billing systems and coding systems to create the patient bill. Healthcare providers must establish charges, code medical records, and bill claims in accordance with charging and billing guidance provided by Medicare and other payers. Pricing for services provided must be accurately and completely loaded, and the CDM must be updated periodically, in a controlled manner, for correct pricing. Clinicians must be trained in how to accurately code and document services provided, and management must monitor charge metrics to enable prompt identification and correction of charge issues. Risks of significance relate to the accuracy and completeness of charges, especially where new technology is in use and where high-dollar procedures and services are involved, such as surgery and cardiology.

Coding

Healthcare systems and providers face growing scrutiny of coding and billing in a quickly changing and increasingly complex regulatory environment. The effective evaluation of ICD-10-CM (clinical modification), ICD-10-PCS (procedure coding system), and Current Procedural Terminology/ Healthcare Common Procedure Coding System (CPT/HCPCS) coding and billing compliance is a challenge that has significant ramifications from a regulatory standpoint as well as for the bottom line of a healthcare system or provider. Common coding challenges include lack of adequate physician documentation and increased workloads due to the complexity of coding guidelines. In addition, third-party coding vendors require regular monitoring for performance and effectiveness.

The top risk areas are presented in alphabetical order first by category and then within each category. They are not ranked.

Denials management

Denied claims result in expensive rework and often lead to lost reimbursement. Healthcare organizations must have procedures for effective denials management and third-party payer follow-up. These procedures should be interdisciplinary, as denials can be caused by numerous processes in multiple departments. Organizations should have an established process to quantify denials by dollar amount, by number of denials, by root cause, and by entity. Additionally, a payment variance process typically is needed to compare amounts received to expected amounts and to identify and correct errors in payments received from contracted payers. Reports summarizing denials activity should be prepared and reviewed periodically by a denials work group that is focused on prevention and root cause analysis.

Patient access

Controls over patient access functions such as patient scheduling, registration, and admission processes must be rigorous to minimize the risk of billing and patient accounting issues, lost revenue, and poor patient and physician satisfaction. Information gathered during the scheduling, preregistration, and registration processes must be complete and accurate, and processes should include checking medical necessity for outpatient services and providing estimates of cost and patient liability. Third-party payers may require certain services to be authorized in advance or precertified, and failure to obtain required authorizations from payers may result in denial of the claim. In addition, insurance benefits should be verified prior to the date of service or soon after to prevent billing delays, and copayments and coinsurance funds should be collected in advance. Finally, financial counselors should visit all uninsured inpatients prior to discharge to discuss patient liabilities, and they should assist patients in identifying and applying for Medicaid and other assistance programs.

What can be done about the risks?

Healthcare organizations' resources are limited even as the number of potential risks grows. To cope with the situation, internal audit departments should take the following steps:

- Review the 23 risk areas identified here.
- Discuss which risk areas apply to their organization.
- Prioritize specific risk areas from highest to lowest risk.
- Channel resources to the top 10 risk areas on the list.

By targeting top risk areas, healthcare organizations can reduce unnecessary expenses that eat away at profitability and financial sustainability.

Learn more

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

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

crowe.com

HC-19005-017A