Through the Risk Lens

Ensuring healthcare organizations achieve expected value from transformation

Healthcare organizations are under pressure to deliver higher-quality care at lower costs: Many health systems are realizing cost efficiencies by instituting enterprise resource planning (ERP) across back office functions from finance to human resources. They are using increasingly disruptive technologies like process automation and digital labor to improve productivity. And, more and more, patient data is being moved to the Cloud to allow electronic health records (EHRs) and other patient data across to be shared across institutions.

This transformation agenda will allow health systems to cut back on waste and duplication and improve margins. Such efforts will free up funds that can be redirected to front-office priorities, such as meeting consumer preferences and improving clinical outcomes. However, as organizations move forward with back office-transformation, it is critical to remember that these efforts may need to be countered with equally aggressive risk management programs.

While most healthcare organizations already have risk mitigation efforts in place, many programs will need to be re-aligned to address emerging risks borne of disruptive processes and technologies. Failing to make this transition may negate the benefits of transformation by introducing the possibility of data loss, reputational damage, regulatory non-compliance and related fines.

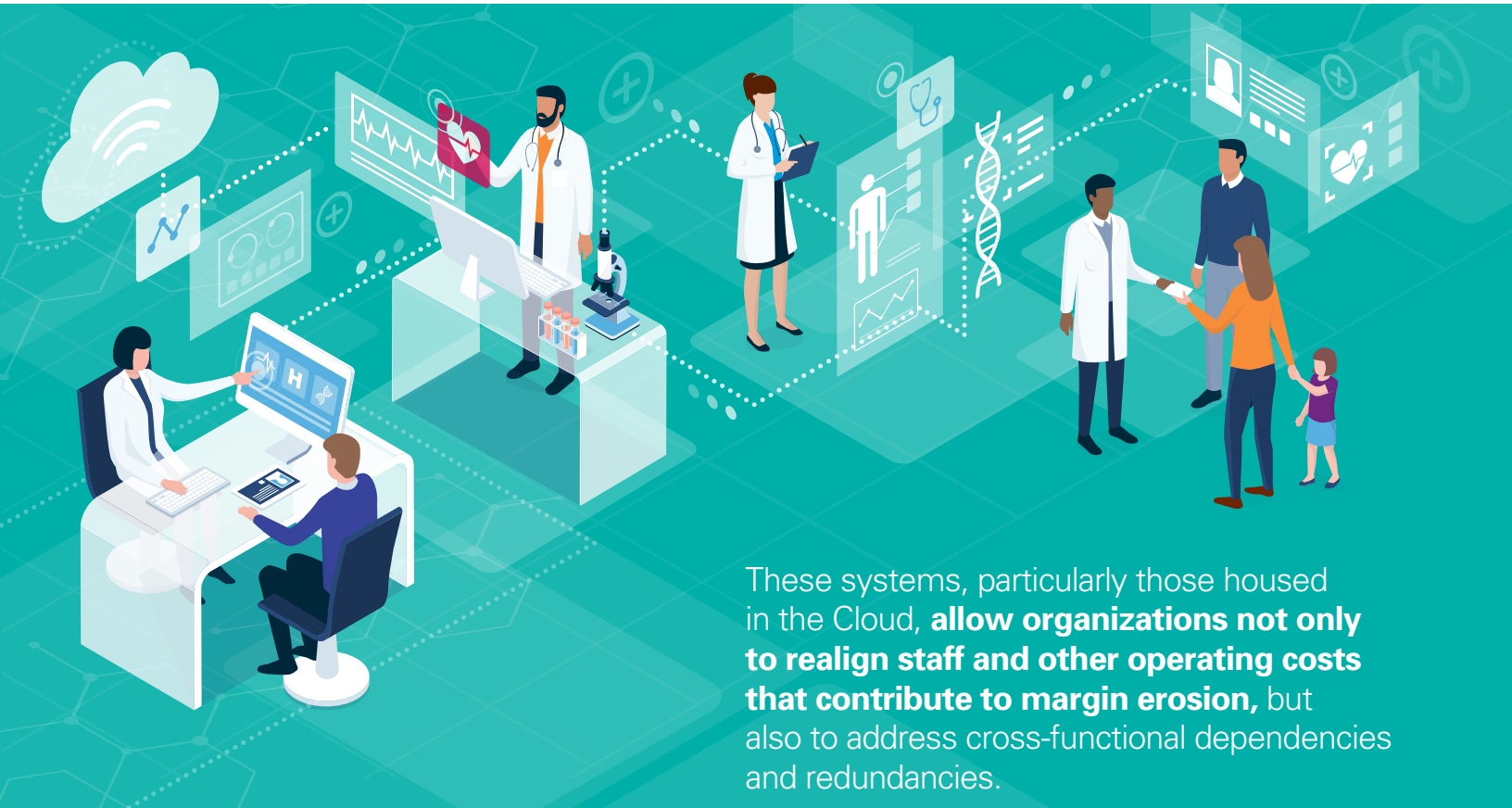
Using ERP to address the total cost of care

The ongoing evolution to value-based care necessitates a better understanding of the total cost of care (TCoC) at healthcare organizations. One way to gain insight into the operating costs associated with an episode of care is by applying ERP and other decision support systems to such back-office functions as finance, revenue cycle, human resources, and supply chain. These systems, particularly those housed in the Cloud, allow organizations not only to realign staff and other operating costs that contribute to margin erosion, but also to address cross-functional dependencies and redundancies.

Although ERP helps organizations *right size* their expenditures, some of this back-office transformation comes with significant risk. For example, time- and cost efficiencies can be achieved in the revenue cycle function by using digital labor, machine learning and artificial intelligence to manage alternative payment arrangements. At the same time, introducing these technologies may increase the risk of data and process anomalies, as well as the possibility that governance and quality may be negatively impacted. Further, as supply chains seek to cut costs by consolidating vendors, renegotiating contracts, and instituting strategic sourcing and automation, they may also raise the possibility of introducing quality and security issues via third parties. Finally, across all ERP and cost takeout efforts, cost-cutting in the back office could potentially have a deleterious impact on patient outcomes if quality suffers as a result.

Through the risk lens
Adopt a holistic approach to transformation

- **Address people and change issues with multifaceted strategies and road maps for the workforce of the future.**
- **Detect cybersecurity and quality risks associated with third-party vendors.**
- **Identify, track, benchmark, and monitor key performance indicators throughout ERP implementations.**
- **Approach cost takeout efforts carefully to avoid negative impacts on internal control and compliance programs.**

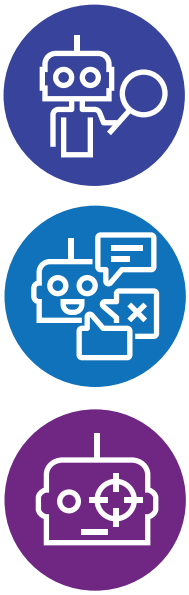


These systems, particularly those housed in the Cloud, **allow organizations not only to realign staff and other operating costs that contribute to margin erosion,** but also to address cross-functional dependencies and redundancies.

Introducing disruptive technologies to gain insights

To analyze the data generated through ERP systems, many organizations are integrating those systems with such advanced technologies as machine learning, predictive analytics, block chain, and more. In addition, many have already made multi-million-dollar information technology investments, a push that is only accelerating with the evolution toward consumer-centric healthcare. Finally, as many health systems pursue mergers and acquisitions as a path to efficiency and scale, new technologies are being introduced through post-deal consolidation and integration efforts.

The insights derived through these technologies – from costs and margins for individual lines of service, to the relationship between cost and quality, to population health patterns – will be critical in value-based care models. At the same time, however, wide-sweeping technology changes can put organizations at risk if their implementations are not managed well and within budget.



Through the risk lens
Establish a transformation integrity process

- **Realize and maintain the expected value and benefits of technology implementations.**
- **Identify priority areas for technological transformation, e.g., process automation, machine learning, cognitive computing, artificial intelligence, and advanced analytics.**
- **Integrate governance, business alignment, change readiness, and technical solution aspects of technology transformation.**

Freeing up patient data for better outcomes

To achieve back-office transformation and keep pace with the evolution to value-based care models, healthcare organizations need to store, utilize, and share large quantities of data. Specifically, analyzing operational data allows organizations to steer dollars and resources toward the most appropriate functional areas. And sharing patient data with individuals and across institutions allows healthcare providers to minimize complications and readmissions, better manage chronic illness, and make predictive insights that can enhance and save lives.

Although Big Data can provide healthcare organizations with critical insights, it is important to marry transformation initiatives with risk evaluation and transparency. This will give organizations the agility to take advantage of opportunities without worrying about whether they are increasing the likelihood of a cybersecurity breach. Since cyber-risks to healthcare organizations have never been higher – with increasingly sophisticated attacks being perpetrated by foreign state-sponsored organizations, hacktivists, and nefarious insiders – cybersecurity teams should be at the table at the beginning of any technology or Big Data initiative.

Through the risk lens
Secure the enterprise first and foremost

- **Transform and mature cyber-security capabilities to align with an increasingly volatile threat landscape.**
- **Upgrade identity and access management to allow access to critical patient data anytime, anywhere.**
- **Maintain information protection agendas as business and technology programs evolve to the Cloud.**
- **Reduce the time frame for detecting and responding to cyber breaches, thus reducing patient risk and reputational damage.**
- **Forensically collect and analyze breach-related data to secure evidence and support legal and law enforcement investigations.**

Why KPMG?

KPMG's risk consulting services include **enterprise risk management (ERM)** to help manage risk across the organization while enhancing and safeguarding value; **third-party governance** and **due diligence programs** to reduce financial, regulatory and operational risks associated with suppliers, partners, care providers and business associates; utilization of **internal audit** as a change agent to address risk challenges, evaluate risk management programs, and influence employee behavior and organizational culture; and anticipation and **compliance with governmental regulations, such as CMS's ICOQR quality mandates, HIPAA, SOC2, FEDRAMP** and more.

In the area of **cybersecurity**, KPMG's highly focused healthcare cyber professionals have assessed leading practices and worked collaboratively with clients to address the most significant risks arising from transformational programs. We provide organizations with integrated advice across the full life-cycle of risk and regulatory change, including compliance and monitoring of new regulations, instituting change management programs during major operational transformations, freeing up data for improved patient care and outcomes while securing attack vectors, and mitigating risks associated with technology transformations, among other services.

KPMG has been recognized as a risk consulting leader in The Forrester Wave™ report, i.e., highest score for Information Security Consulting Services and tied for highest score for strategy.

To learn more visit us at: kpmg.com/us/healthcarelifesciencesinstitutes

Contact us

Karen Vangyia
Partner, Healthcare Risk Consulting Leader
kvangyia@kpmg.com
314-244-4022

Wayne Cafran
Principal, Healthcare Risk Consulting
wcafran@kpmg.com
212-909-5394

Carl Kriebel
Managing Director, Healthcare Cyber Security
ckriebel@kpmg.com
412-391-9710

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia