Deloitte. Insights

A report by the Deloitte Center for Health Solutions

Health care risk leaders are keeping their heads above water for now

But a tidal wave of new risks may force them to sink or swim

Deloitte Risk and Financial Advisory helps organizations effectively navigate business risks and opportunities—from strategic, reputation, and financial risks to operational, cyber, and regulatory risks—to gain competitive advantage. We apply our experience in ongoing business operations and corporate life cycle. We leverage next-generation solutions in our Ventures Fund and Managed Services and Products business to help clients become stronger and more resilient. Our market-leading teams help clients embrace complexity to accelerate performance, disrupt through innovation, and lead in their industries. For more information on our Risk and Financial Advisory services, visit www.deloitte.com/us/risk.

Contents

Executive summary

WITH THE AIM of understanding the level of alignment and prioritization that health systems and health plans have on organizational risks now and in the future, the Deloitte Center for Health Solutions recently surveyed health system and health plan chief financial officers (CFOs) and interviewed risk leaders (chief risk officers [CROs], chief audit executives, and chief compliance officers). Our findings offer insights into emerging opportunities to manage risk through collaboration and investment, and we offer suggestions on how health care organizations can prepare for the future, starting today.

Our research showed that CFOs and risk leaders at health care organizations are at present generally aligned on managing key risk areas and believe they are prepared. CFO priority areas are consumer engagement, cybersecurity, transitioning to value-based care, and technology and digital business transformation, while cybersecurity, privacy, and patient safety are the focus areas for risk leaders.

However, there are some early indicators that the risk functions at these health care organizations lack the capacity (talent, organizational flexibility, technology) or the time to prepare for the type and pace of change the health care industry is likely to experience in the coming years.

- For top priority risks, the majority of CFOs say they are either only moderately or not prepared for the future:
  - Cybersecurity (65 percent);
  - Transition to value-based care (58 percent);
  - Consumer engagement (58 percent); and
  - Technology and digital transformation (58 percent).
- CFOs noted that challenges to preparing for future risks include:
  - Allocation of resources based on historical risk experiences (48 percent);
  - More important organizational priorities (38 percent); and
  - Lack of information or awareness (30 percent).

- Risk leaders said that crisis management today prevents them from planning for the future.

- Budgets also are narrowly concentrated on the top risks.
  - Fifty-six percent of CFOs indicate that they spend half or more of their budget on their top three risks while 62 percent expect the percentage of the risk budget allocated to their top priorities to grow disproportionally larger over the next few years.

How can risk functions (compliance, legal, and internal audit) be more prepared and agile to enable their organizations' strategies and even embrace these key risks versus just reacting to them? How can organizations prevent their risk functions from failing? We offer suggestions for the steps health plans or health systems can take to keep up with the changing demands and thereby focus on opportunities. These include an action plan that begins with educating leaders and then the broader organization about the impact of emerging technologies, developing an inventory of current and proposed strategies and technology investments, establishing policies for the use and monitoring of emerging technologies, and assessing the skills and capabilities of risk staff to ensure that they align with risk programs for these new investments.

Introduction

THE RISK LANDSCAPE for health care organizations is continuously shifting and expanding. In addition to daily challenges such as compliance, patient safety, and cybersecurity, organizations often have to grapple with disruption to the industry, increasing consumer demands, and innovation-driven changes via both scientific discoveries and emerging technologies. While these latter issues may be raised in strategic planning agendas at most health care organizations, they are not always considered from a risk perspective.

Some of these risks overlap with each other—investing in new technologies requires expanded cybersecurity efforts. Old risks can also manifest in new ways; for example, as health care organizations continue to invest in emerging technologies, they should now consider new potential concerns such as data dichotomy, algorithm appropriateness, and the "next generation" of cybersecurity that is more complex than today. (See the sidebar, "Monitoring traditional risk with forward-thinking approaches.")

We found that health care organizations are able to keep up and balance efforts against top risk areas today. But, we identified some early indicators that their risk functions may lack capacity (skill, people, time) to deal with the type and pace of change expected in the coming years. A tidal wave of new risks may force them to sink or swim. Today's models may not be able to take on new, more complicated risks in the future even though these opportunities are critical for the enterprise.

RESEARCH METHODOLOGY

To better understand how health care organizations are navigating today's ever-more complicated risk landscape and preparing for the future, the Deloitte Center for Health Solutions researched how health care organizations prioritize and deploy resources to their top risks. We conducted a survey of 40 CFOs, as some CFOs oversee board committees or budgets dedicated to risk management. For comparison, we also interviewed 15 risk leaders including CROs and C-suite and VP-level leaders from the risk functions (compliance, legal, and internal audit) of health systems and health plans. We wanted to compare both the strategic and tactical approaches to risk. Health system participants were from organizations with an annual income of more than US$2.5 billion. Health plan participants were from organizations with more than 500,000 covered lives.

Risk priorities include a mix of familiar and emerging concerns

WE ASKED CFOS and risk leaders, separately, what their top organizational risk priorities were. Our findings highlight how health care organizations prioritize a mix of familiar and emerging concerns. While there are some differences in the two perspectives, there are similarities, too. CFOs ranked their top risk priorities today as (see figure 1):

- Consumer engagement (58 percent);
- Cybersecurity (55 percent);
- Transitioning to value-based care (55 percent); and
- Technology/digital transformation (53 percent).

Technology and digital transformation (including artificial intelligence [AI], cognitive computing, and other emerging technologies) and big data/analytics (the ability to report on performance metrics, integrate multiple internal data sets for data-driven insights, or leverage external data sets on consumer preferences and social determinants of health for clinical and business decisions) are particularly interesting as risk priorities. CFOs expect these to increase significantly in priority over time:

- Technology and digital transformation (79 percent rate it a top risk in three years vs. 53 percent today); and
- Big data/analytics (54 percent rate it a top risk in three years vs. 30 percent today).

Both these areas are also connected to broader strategies and investments that health care organizations are making to become more efficient, engage consumers, stay competitive, and, most importantly, remain relevant in their markets. The ability to better engage consumers, improve cost and quality of care, and transform their businesses, all depend on the ability to leverage technologies, digital solutions, and data-driven insights. But these investments also carry cyber, regulatory, quality, safety, and other strategic risks that organizations should prepare for.

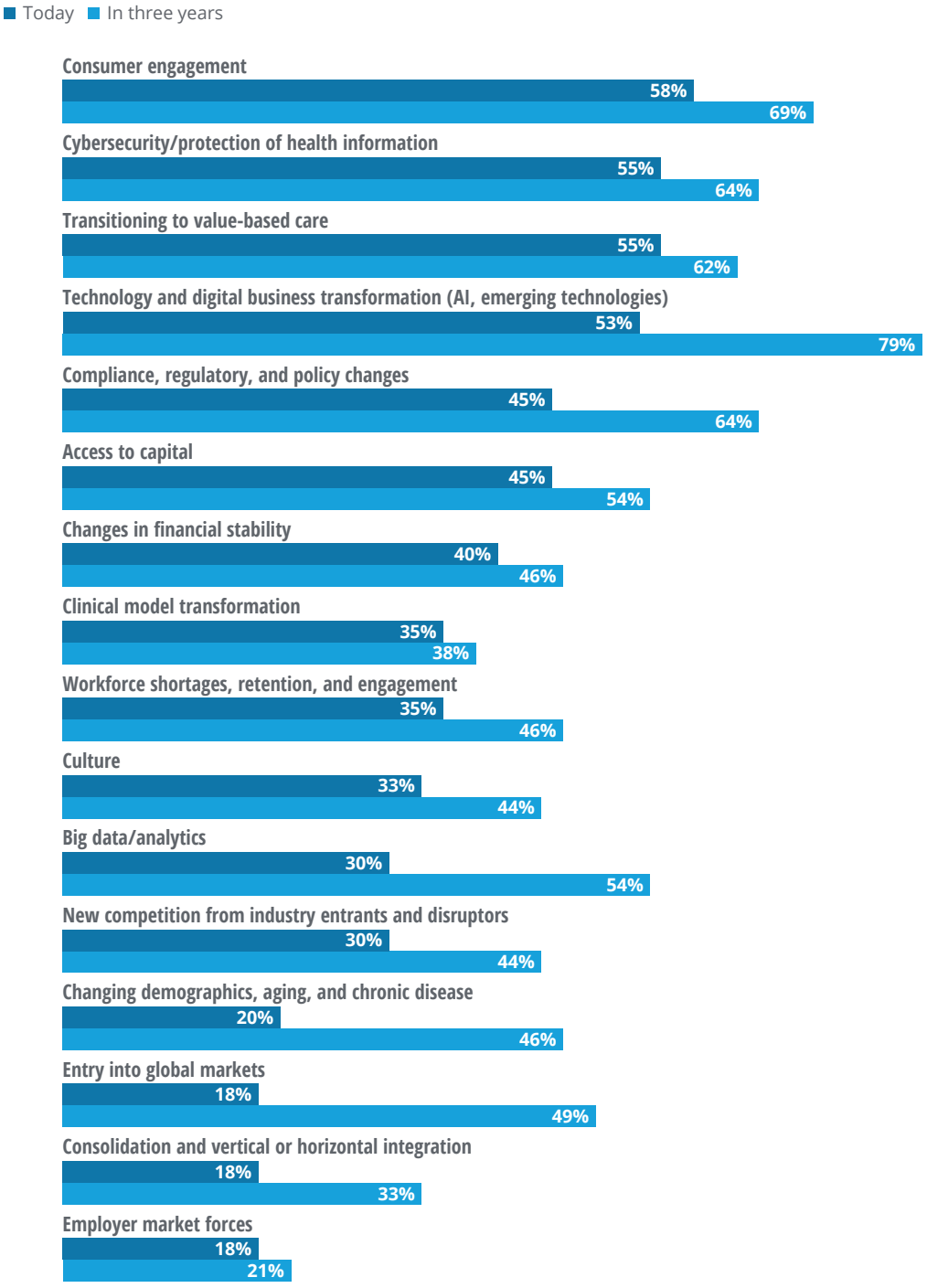
Some surprising and less familiar areas of emerging focus include the potential for entry into global markets (18 percent say it is a top priority today vs. 49 percent in three years) and changing demographics, aging, and chronic disease (20 percent say it is a top priority today vs. 46 percent in three years). Demographic changes and chronic disease have been familiar topics for the strategy and operations teams in many organizations. However, some of the efforts in these areas involve new partnerships and alliances with other health care stakeholders that directly impact how risks can be experienced and who is responsible for managing them. Reassessing risk profiles in key initiatives and designing in risk management from the start will help avoid surprises later. Entry into global markets brings risk considerations (which other industries have been effectively managing for some time) and entail a rapid learning curve for health care on key global risk topics—areas such as Foreign Corrupt Practices regulation, cultural and economic differences, and the complex system of global privacy regulations different from those in the United States.

How do these priorities from CFOs line up with those of risk professionals? In our in-depth discussions with risk leaders, we found that their top risk priorities (and where they have focused most of their resources—dollars and people) include cyber/data security, privacy/Health Insurance Portability

FIGURE 1

Consumer engagement is the top priority risk at health care organizations according to CFOs, but technology and digital transformation will be the top priority risk in three years

Top priority risks faced today vs. in three years



Note: Responses to the question: "How would you rate each of the risks that faces your organization today vs. in three years? Please rate the priority level for each source of risk." On a scale of 1 (not a priority) to 10 (high priority), the chart shows an aggregate of top three ratings (8, 9, and 10).

Source: 2018 Deloitte Health Care CFO Risk Management Survey.

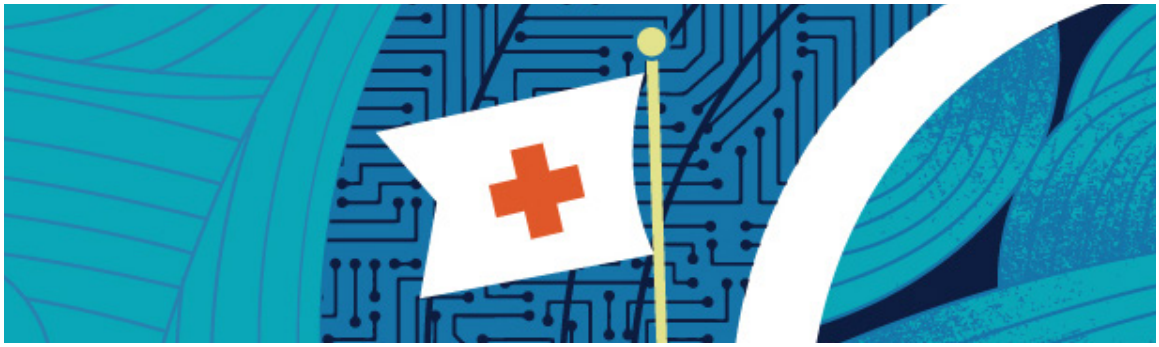
> **"At the end of the day, we have to focus on our core capabilities—that is, data. Therefore, cyber prevention will always be critical."**
>
> — ***Health plan risk executive***

and Accountability Act (HIPAA) (with technology and staff), and patient safety.

These are issues that risk leaders have been managing for many years, but they are growing in breadth and reach. New technologies are changing the risk profile for these topics and prompting the addition of new solutions. They are also more imminent today because organizational strategies that include consumer engagement, value-based care, and digital transformation all amplify cybersecurity, privacy, and patient safety risks. Risk leaders also noted that their organizations are becoming more complicated through M&A and expansion.

The speed of transformation at health care organizations is accelerating. Nontraditional players have been entering the market at a rapid pace, and competition from these sources is expected to grow. Scrutiny of costs and quality of care are rising. Thousands of innovative solutions that enable consumer experience have been introduced in the marketplace. The result is greater competition for shrinking revenue and margins. Organizations should determine their path to survive the industry's current transformation.[1] All this means that risks are also increasing at an accelerating pace.

Taking a new approach with risk priorities



IN THE PAST, prevention and limiting access was the primary method of mitigating risks, particularly with technologies such as personal devices or patient records. But, the scope and type of challenges have changed with technological advances. At the same time, regulatory and consumer expectations about access to information are significantly different today. These market pressures and strategies likely require a new approach to enabling access while mitigating risk.

"With technology and risks, what is old is new again. The pendulum is swinging back. HIPAA and privacy are a major concern just like 20 years ago."

— ***Health plan risk executive***

While these issues may seem old and familiar, their magnitude and the approaches to address them are not the same. Convergence, regulatory innovation (payment and coverage reform), consumer influence, and other pressures are beginning to drive major waves of innovation and transformation for the industry. While executives at some organizations have had these topics on their radar for at least two years, others are currently developing and implementing strategies to deal with them. Risk functions likely should engage more as these strategic decisions are being made.

Looking ahead, the risks in these areas will continue to evolve and become more complicated. A digitally enabled, interconnected health care system will require risk management to not only enable this but also to monitor and respond with real-time diligence. Organizations should leverage lessons learned and bring a whole new thought process to the table. A key question is: Can they do so effectively if they are at capacity covering current risks? Also, do they have the talent and skills to meaningfully do so?

MONITORING TRADITIONAL RISK WITH FORWARD-THINKING APPROACHES

Emerging technologies promise to help transform health care organizations. Technologies like AI, robotic process automation (RPA), cognitive computing, and others can help create efficiencies, improve clinical decision-making, and better engage consumers.

While the majority of organizations have enabling technologies in place, only about a third of CFOs indicate that they are leveraging emerging technologies for their risk functions:

- Sixty-three percent of organizations have invested in supporting technologies for risk-tracking and processes;
- Thirty-eight percent have developed data analytics and other emerging technologies for risk identification; and
- Thirty percent currently leverage AI or other emerging technologies for sensing and identifying risks. Another 45 percent say that they plan to do so in the next three years (25 percent have no plans).

Auditing and monitoring innovation—The use of advanced data analytics over traditional internal audit approaches may improve an organization's ability to identify and manage risk

Monitoring of regulatory and operational risk elements using advanced data analytics, RPA, and other emerging technologies can reduce an organization's reliance on the traditional, labor-intensive approach, allowing for better risk management and reducing long-term costs. Automated solutions allow for the analysis of a much larger universe of transactions, enabling the organization to better identify anomalies, regulatory and operational risk, and performance trends. Near real-time feedback could help organizations identify and correct instances of noncompliance and operational errors in time, more importantly, in advance of a regulatory audit. As robotic tools learn and understand data, deeper insights and understanding of risks can be identified and further inform the refinement of data modeling and algorithms.

Risk factors to be considered

- **Administrative enforcement actions, sanctions, and fines** from regulators such as CMS for failure to meet program audit requirements. These can take the form of financial penalties, suspension of enrollment, and, if warranted, plan disbarment.
- **Reduction in revenue** based on poor audit performance including the CMS Star Rating Program and related measures, as well as data quality issues that impact plan revenue, such as encounter and claims data submitted to federal and state regulators.
- **Cost of human resource capital** needed to address and respond to regulatory oversight, including the development of and monitoring against remediation plans, corrective action plans, root cause and member impact analysis, and the need to conduct follow-on audits to confirm remediation.

Prepared for now, but prepared enough for the long term?

WHEN ASKED ABOUT their level of preparedness, some CFOs reported (see figure 2) feeling very prepared for their top priority risks. However, when all priority areas are considered, it was most common for them to report they were only moderately prepared, and in some of the areas of emerging importance, a significant percentage said they were not prepared at all.

Most CFOs say they are either only moderately or not prepared in:

- Consumer engagement (58 percent);
- Technology and digital transformation (58 percent);
- Transitioning to value-based care (58 percent); and
- Cyber (65 percent).

Risk leaders also painted a nuanced picture of their level of preparedness. They felt prepared for their priority risks, but they also describe departments that are thinly staffed and say that they tend to devote significant time to crisis management—investigating potential HIPAA breaches, patient/member complaints, and patient safety issues.

Also, some health systems and health plans are currently not focusing beyond the immediate steps to prepare for risks. While most (73 percent) of the CFOs said they have identified staff to address risks, fewer have invested in supporting technologies (63 percent) to prepare for risks or conducted training (58 percent) (see figure 3).

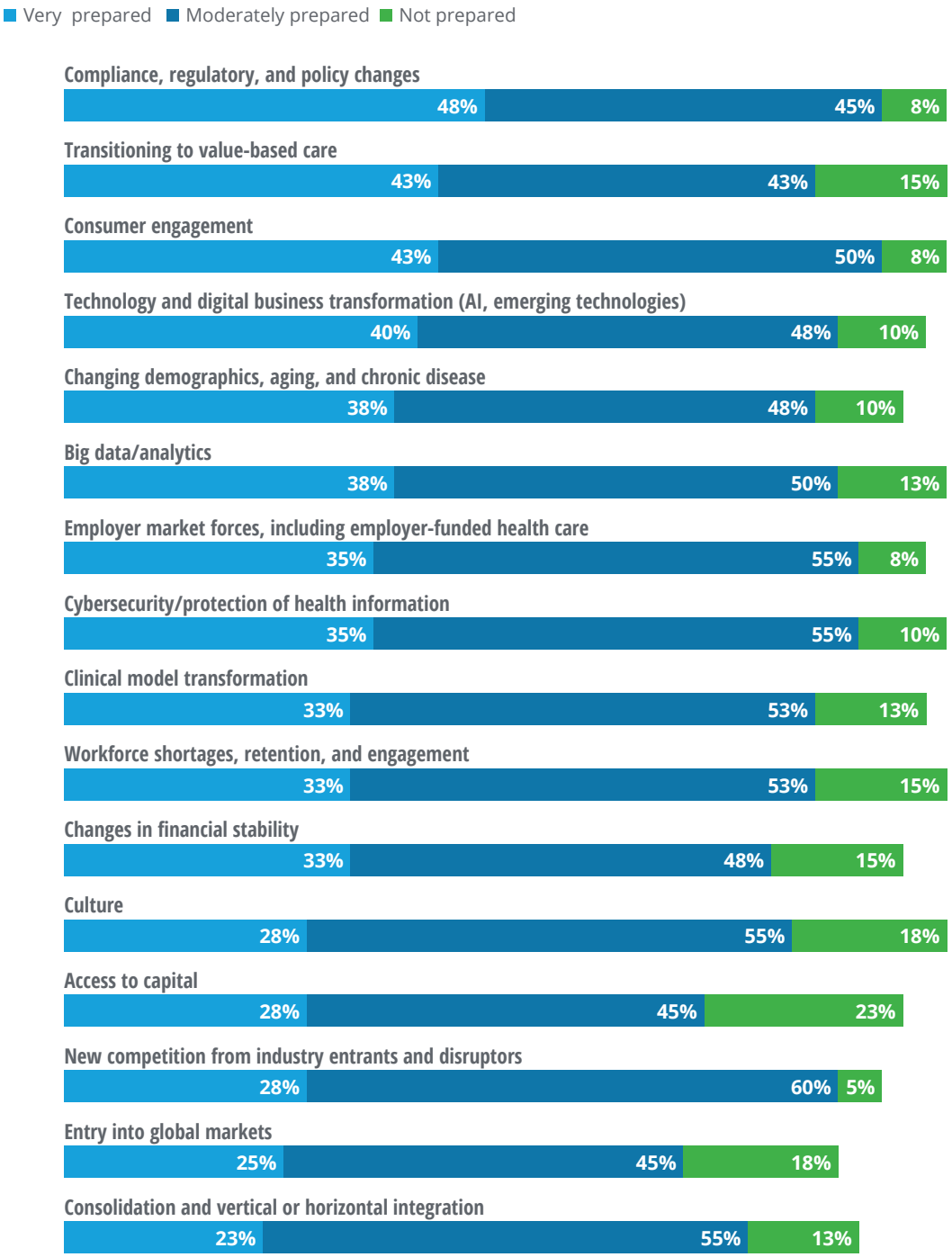
"Risk managers put out fires."

— ***Health system risk leader***

FIGURE 2

Nearly half of CFOs indicate that they are very prepared for their priority risks

Level of preparedness for risks



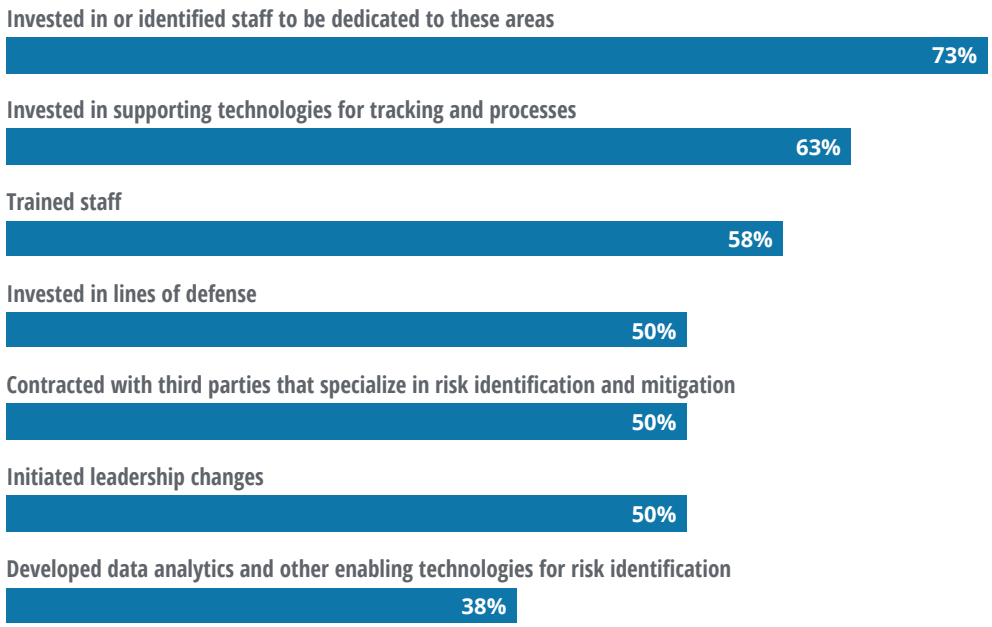
Note: Data is in response to the question, "How prepared is your organization today for each of these risks?" Not applicable responses are not included and therefore some percentages do not total 100 percent.

Source: 2018 Deloitte Health Care CFO Risk Management Survey.

FIGURE 3

To prepare for risks, a majority of surveyed CFOs (73 percent) have identified staff to address risks

Top risk preparation activities



Note: Data is in response to the question, "What have you specifically done to prepare your organization for these risks?"
Source: 2018 Deloitte Health Care CFO Risk Management Survey.

Barriers to preparing for the future

"The target is always moving"

— *Health system risk executive*

CFOS NOTED THAT the top challenges their organization faces in identifying and responding to potential risks include allocation of resources based on historical risk experiences (48 percent), more important organizational priorities (38 percent), and lack of information or awareness (30 percent) (see figure 4). Risk leaders discussed how challenging it is to be prepared for the unknown when it comes to risk management for broader strategic topics like disrupters to the marketplace or business transformation. They also said they tend to have a short-term perspective and find it challenging to focus on longer-term risks due to:

- Never-ending day-to-day tasks related to compliance (such as tracking down misdirected faxes and HIPAA breaches or member/patient complaints);
- Recent cyberattacks or patient safety issues; and
- The changing regulatory landscape.

FIGURE 4

Nearly half of organizations allocate resources for risk management based on historical experiences

Top barriers to identifying and responding to potential risks

Note: Data is in response to the question, "What are the top barriers to identifying and responding to potential risks to your organization?"

Source: 2018 Deloitte Health Care CFO Risk Management Survey.

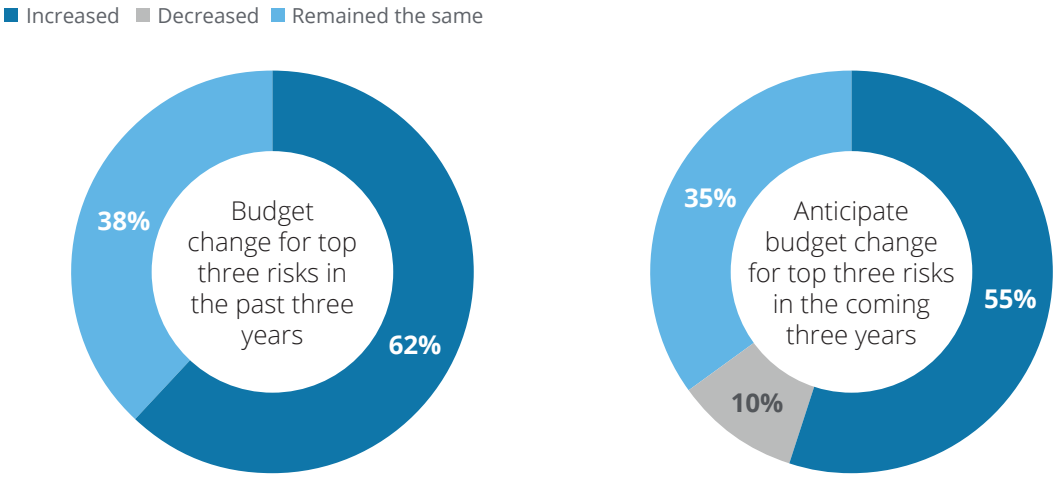
Allocation of resources

WHILE BUDGETS ARE being allocated, organizations' level of preparedness for new risks may not change, as they may be using budgets for problems in the rear-view mirror rather than those on the horizon. As mentioned earlier, 48 percent of CFOs admitted that resource allocation is based on historical risk experiences (figure 4).

According to our research, 56 percent of CFOs indicate that they spend half or more of their budget on their top three risks and 62 percent indicated that their budget for the top three risks has grown in the past three years (figure 5). Another 55 percent expect their budget for their top three risks to grow in the next three years. However, even with these increases, organizations may still be spread too thin; besides, they are focused too narrowly, as indicated by the portion who spend more than half their budget on their top three risks.

FIGURE 5

Budgets have grown during the past three years for top risk priorities and are expected to continue to grow in the next three years



Note: Data is in response to the questions, "Has the amount of budget changed for your top three risk priorities in the past three years?" and "Do you anticipate your budget to change for your top three risk priorities in the next three years?"
Source: 2018 Deloitte Health Care CFO Risk Management Survey.

EMERGING TECHNOLOGIES CARRY NEW AND CHALLENGING RISKS

The following use cases are intended to show that while emerging technologies represent exciting innovations for health care organizations, they also carry new and challenging risks. They highlight how a risk approach that creates more capacity and still effectively manages the risk is more useful than a rear-view mirror approach.

Use case 1: Data dichotomy—Managing data risks allows organizations to harness data analytics to improve decision-making[2]

The ability of data to aid decision-making is transforming health care. From behavioral data to social determinants of health, the types of unique data being collected to drive organizational efficiencies and competitive advantage are immense. Organizations are striving to accelerate innovation and drive personalization of services using data-driven insights and to capitalize on its increasing value by monetizing it. However, the lack of standardized practices for collection, storage, and exchange is a challenge to data integrity and accuracy. Further, aggregating data from new and diverse sources—medical apps, smart wearables, social media portals—raises concerns about privacy and transparency. It also raises fundamental new questions: How to prepare for the reality that consumers may give consent for convenience but not understand what data is collected and how it is used.

Additionally, exchanging data in a distributed ecosystem with inadequate governance mechanisms increases quality, security, and confidentiality issues. Organizations that implement strong data quality and security strategies can gain the trust of patients, regulators, and ecosystem partners and reap significant benefits.

Risks factors to be considered

- **Loss of reputation and public trust** in an environment where consumer expectations and understanding, as well as regulatory guidelines on data use, are changing rapidly.
- **Potential patient safety concerns and financial loss due to inaccurate business decisions made** using outputs of analytical models developed on unreliable or inaccurate data (for example, health systems could have concerns regarding patient outcomes or suffer heavy losses from inaccurate patient data used for treatment decision-making).
- **Noncompliance with regulations** such as General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Medicare Access and CHIP Reauthorization Act (MACRA), and HIPAA, resulting in regulatory actions such as fines, more frequent inspections, suspension of product approvals, and import bans. Proposed Centers for Medicare and Medicaid Services (CMS) rules on information blocking also mean that simply saying "no" to sharing health information with others isn't always an option. Please see the Deloitte Center for Regulatory Strategy blog for further information on the proposed rules.
- **Operational challenges** from additional time and resources spent on cleaning and reconciling disparate data, especially for businesses that monetize data aggregated from multiple sources to provide a full picture of patient health.

Use case 2: Algorithm appropriateness—Curtailing algorithmic bias and increasing transparency can accelerate new capabilities and insights[3]

AI and intelligent automation are radically altering health care by helping enable better decision-making and driving efficiencies. However, the black-box nature of these self-learning algorithms can make them difficult to understand and manage. Algorithms are prone to human biases and faulty assumptions, and risks could be compounded by erroneous training data, unsuitable modeling techniques, and incorrect interpretation of algorithmic outputs. As algorithms become more pervasive and complex, organizations should adopt a risk-aware mindset to effectively manage the novel risks emerging from cognitive technologies.[4] In doing so, they can reap immense benefits and provide more effective and personalized services to patients.

Risks factors to be considered

- **Threat to patient safety caused by erroneous diagnosis and treatment** (for example, incorrect recommendations by science and insights engine businesses that use automated diagnostic applications lacking contextual data).
- **Legal actions and reputational damage** as a result of decisions made by algorithms, not aligned to legal, cultural, and ethical norms (for example, racial profiling by health "chatbots" used by businesses to tap into patient data for the generation of personalized health insurance offerings).
- **Unvalidated AI algorithms** and baseline data sets used too early in their development, resulting in incorrect decisions and hindering the adoption of beneficial and potentially life-saving technologies by enterprises and patients when they are better developed.

Rethinking today's risk approach

THE SURVEY RESULTS and use cases highlight that while risk functions at organizations are managing today's risks, a fresh approach to risk management may be needed.

The potential to force risk functions to sink or swim

The industry may have reached a point where risk functions are barely keeping their heads above water and just keeping up. A tidal wave of new risks for the health care industry has the potential to rapidly bring new changes and challenges. Without changing how they approach risk, at what point will the risk function **be forced to sink or swim**—meaning it will be unprepared to address the magnitude and type of future risks? How do well-resourced enterprises protect themselves in an interconnected data-driven health care system?

Why a risk approach with emerging technologies cannot wait

As emerging technologies become more pervasive at organizations, they should be accompanied by a risk approach that builds technical capacity while effectively managing today's top-of-mind risks. Technology is changing and maturing exponentially; to start behind the curve today will only make it more difficult to catch up later. By taking the time now to consider how to thoughtfully deploy new technologies, organizations can prepare for today's risks and those of the future. Waiting to do this can result in greater, more complicated risks as organizations will have already started to invest in and use these new technologies.

Furthermore, risk departments should understand that the underlying components of emerging technologies—models and algorithms—while important, carry risks within themselves. These models will likely become more pervasive in the organization, helping to determine financial, business, and clinical decision-making. The more these decisions rely on these technologies and their underlying programming, the greater the risks and impact. These "black boxes" cloud the factors that create the outputs and could be potentially inaccurate, as the models themselves or the data that the models are built on are vulnerable to accidental or intentional biases, errors, or fraud. An example of algorithms that are still under development includes how the same person with identical saliva samples received different ancestry results from different genetic testing services.[5]

Organizations should test these models for accuracy, appropriate use, and protection from cyberattacks. Organizations leveraging bots, for example, should put in place policies, processes, and tracking procedures to prevent the bot from proliferating errors.

How to move forward and keep swimming above water

As a start, risk leaders should take ownership of educating the broader organization on potential

risks with emerging technologies. This approach can help them get their foot in the door and be seen as enablers of strategies. Enhancing the organization's knowledge and maturity can help position risk leaders as partners on initiatives for emerging technologies.

Other action steps for risk leaders to consider include:

- **Creating an inventory** of the technologies, models, and algorithms being used throughout the organization; understanding the organization's reliance on them; and evaluating the potential impact if they don't function properly.
- **Using a governance framework** involving appropriate risk leaders, business and operations leaders, and board committees to identify opportunities for emerging technologies, assessing the models behind the technologies, and ensuring that a risk perspective is included when developing and using the solutions and processes for the technologies. Return on investment and risk should be assessed together.
- **Establishing policies and procedures** for the use of these technologies, models, and algorithms.
- **Continuously testing, monitoring, and validating technologies, models, and algorithms** both before and after they are implemented. This should include documentation of testing procedures and independent reviews of the testing performed by sampling test cases documented, results generated, and issues logged.
- **Assessing the skills and capabilities of staff in risk functions** to ensure that they have the knowledge and understanding of emerging technologies, models, algorithms, and other new strategies to lead the risk programs in these areas; educating current staff or recruiting staff to gain that knowledge and capability.

Once risk leaders have the inventory and baseline processes and governance in place, the focus should be on maturing the risk function and maintaining risk programs. Additional action steps include:

- **Performing an annual recertification** of the design and implementation of automation technologies, a process which should also be tested to provide objective assurance that it's working effectively;
- **Random testing** of technologies, models, and algorithms to help ensure that they are still performing correctly; and
- **Creating your own risk organization strategy and vision** for how you will leverage and implement these technologies for your own functions.

Instead of using a rear-view mirror approach, much of this requires the risk function to "build the car while driving it." Parallel workstreams should include:

- Piloting and building emerging technology applications to show progress and test the process;
- Identifying use cases for opportunities with emerging technology for the future; and
- Adapting the operating model to sustain the piloted approaches.

The reality is that today's risk functions don't have the bandwidth, capabilities, and skills to move forward effectively. Risk leaders need additional resources and should build the business case for them immediately.

Endnotes

1. David Biel, Maulesh Shukla, and Claire Boozer Cruse, *The health plan of tomorrow: Business model transformation is the only way to adapt to disruption*, Deloitte Insights, February 7, 2019.
2. Amry Junaideen et al., *Harnessing opportunities and managing risk in the future of health*, Deloitte, 2019.
3. Ibid.
4. A field of computer science that mimics functions of the human brain.
5. Rafi Letzter, "I took 9 different commercial DNA tests and got 6 different results," Live Science, November 5, 2018.

About the authors

AMY KROLL, Deloitte & Touche LLP, is a principal and the health care sector leader within Deloitte's Risk and Financial Advisory practice. She has more than 20 years of experience assisting clients by improving their governance, operations, and risk management processes. She advises clients on integrated risk management strategies and assessment frameworks focused on effective risk management and efficient use of resources. She holds a BSBA, management information systems, from the University of Minnesota Carlson School of Management. She is based in Minneapolis.

CHRISTINE CHANG, Deloitte Services LP, is a research manager with the Deloitte Center for Health Solutions. She conducts primary and secondary research and analysis on emerging trends, challenges, and opportunities within the health care system. Prior to Deloitte, she provided consulting services to health care stakeholders and researched the health information technology market. She holds an AB from Princeton University and an MPH from the Mailman School of Public Health at Columbia University. She is based in New York.

WENDY GERHARDT, Deloitte Services LP, is a senior manager with the Deloitte Center for Health Solutions. She is responsible for conducting research to inform health care system stakeholders about emerging trends, challenges, and opportunities. Prior to Deloitte, she held multiple roles of increasing responsibility in strategy/planning for a health system and research for health care industry information solutions. She holds a BBA from the University of Michigan and an MA in health policy from Northwestern University. She is based in Detroit.

Acknowledgments

PROJECT TEAM

April Patterson helped shape the research and recommendations through her expertise and guidance. **Satish Nelanuthula**, **Srinivasarao Oguri**, and **Soumya Mohapatra** analyzed the survey results.

The authors would like to thank **Amry Junaideen**, **Simon Gisby**, **Jacqi Fifer**, **Claudia Douglass**, **Garrett O'Brien**, **Tim McAndrews**, **Lindsey Hennessy**, **Cliff Goss**, **Mike Schor**, **Jack Scott**, **Kelly Sauders**, **Julie Hamilton**, **Michelle Fleming**, **Lauren Wallace**, **Samantha Gordon**, and the many others who contributed to the success of this project.

About the Deloitte Center for Health Solutions

The source for fresh perspectives in health care: The Deloitte Center for Health Solutions (DCHS), part of Deloitte LLP's Life Sciences and Health Care practice, looks deeper at the biggest industry issues and provides new thinking around complex challenges. Cutting-edge research and thought-provoking analysis give our clients the insights they need to see things differently and address the changing landscape. To learn more about the DCHS and our research, please visit www.deloitte.com/centerforhealthsolutions.

Contacts

Amy Kroll
Health Care Advisory Practice leader
Principal
Deloitte & Touche LLP
+1 612 692 7173
amykroll@deloitte.com

Sarah Thomas, MS
Managing director
Deloitte Center for Health Solutions
Deloitte Services LP
+1 202 220 2749
sarthomas@deloitte.com

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Ramani Moses, Blythe Hurley, Nairita Gangopadhyay, and Abrar Khan

Creative: Sonya Vasilieff and Rajesh Venkataraju

Promotion: Alexandra Kawecki

Cover artwork: Sonya Vasilieff

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

About Deloitte