protiviti®

Face the Future with Confidence

Addressing Priorities for Internal Auditors in Healthcare Delivery Organizations

Next-Gen Internal Audit in Healthcare — Focusing on Innovation and Transformation

While internal audit functions at healthcare providers are committing to a next-generation operating model, more progress is still needed to reach an optimal state.

Healthcare providers are transforming — both in the nature of care they deliver and their operations. They continue to innovate and develop new ways to increase the length and quality of their patients' lives. As this commitment extends throughout their organizations, the organizational transformation will create a new set of strategic challenges for internal audit functions to address in the coming decades. In fact, our view is that now is the time for internal audit functions to evolve into a next-generation internal audit function.

For healthcare providers, making good on the "triple aim" of increasing the quality of patient care, improving population health outcomes, and curtailing medical costs requires them to pursue multiple priorities. These include accessing and leveraging more and better data and analytics, fortifying information security capabilities, advancing relationships with third-party partners to improve the continuum of care, addressing changing talent management needs, complying with ongoing regulatory requirements, leveraging new technology, and more.

The industry's focus on advanced technologies, along with a range of related innovations, are driving the need for internal audit innovation and transformation. While internal audit advancements are progressing, the pace of change is not keeping up with organizational needs, according to the healthcare provider results from Protiviti's 2019 survey on internal audit capabilities and needs.[1]

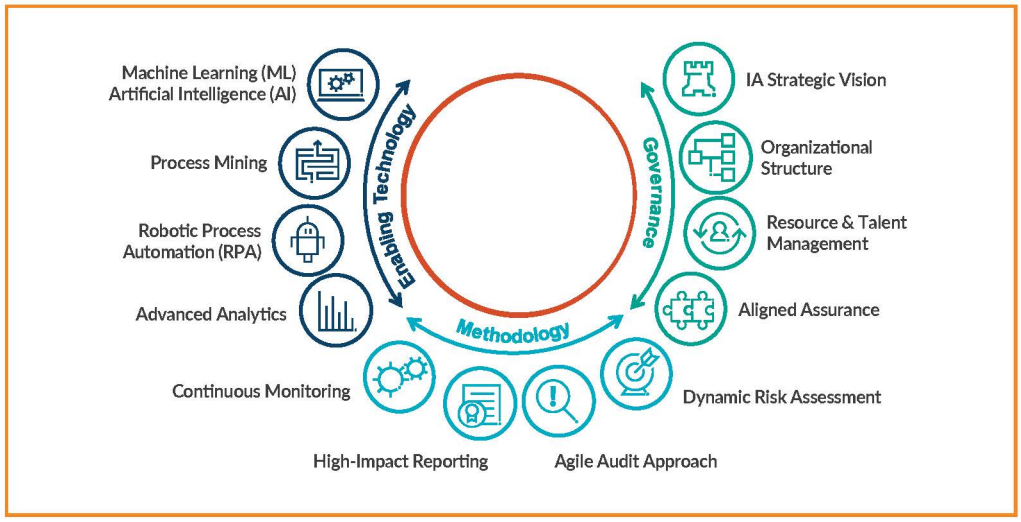
In addition to revealing the top internal audit priorities, this year's findings make it clear that it is time for leaders of internal audit functions to commit to the investment and deployment of emerging technologies, innovative approaches, and instilling throughout their ranks a commitment to operating as a next-generation internal audit function.

[1] While this paper focuses on healthcare industry findings, for more information about the overall findings for all industries, read our full survey report, *Embracing the Next Generation of Internal Auditing*, available at www.protiviti.com/IAsurvey.

Now Is the Time for Next-Generation Internal Auditing

Healthcare providers are far from the only segment of organizations confronting a mandate for change. As Brian Christensen, Protiviti's Executive Vice President of Global Internal Audit, notes: "There needs to be a fundamental rethinking of the design and capabilities of the internal audit function to be more forward-looking and help improve the business." This is articulated in our white paper, *The Next Generation of Internal Auditing – Are You Ready?* [2] In this paper, we advocate that internal audit functions need to perform their work in a more agile manner and detail how they can leverage the proliferation of data combined with technology-enabling auditing solutions to deliver on this transformational objective. The need for this new mindset applies across all three categories of our next-generation internal audit model: governance, methodology and enabling technology.

Protiviti's Vision: The Next Generation of Internal Auditing



[2] *The Next Generation of Internal Auditing – Are You Ready?* Protiviti, 2018, www.protiviti.com/auditnextgen.

Internal audit functions across all industries are developing and adopting next-generation internal audit competencies, including agile auditing, artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), and continuous monitoring, among other innovative capabilities. In our aforementioned 2019 survey on internal audit capabilities and needs, we devoted a special section to assess how internal audit functions at healthcare providers are progressing on their next-generation journeys.

On that count, it is encouraging to find that, according to our results, a strong majority of healthcare provider respondents have increased their focus over the past 12 months on innovation and transformation initiatives to support audits. It is also promising that among internal audit functions with data analytics groups, most plan to increase headcount in those groups during the coming year.

However, our results also suggest more progress is still needed. For example, compared to other industries, internal audit functions at healthcare providers significantly lag in progress around innovation and transformation initiatives.

Tough obstacles exist along internal audit's next-generation journey. Scant time and ever-increasing workloads impede progress. There also exists a perception among some organizations that innovation and transformation are not new mandates, but simply the latest in a procession of new technology-tool-adoption requirements stretching back to meaningful use. Yet, these impediments also underscore the essential need for internal audit transformation while pointing to opportunities for progress. The time constraints many internal audit functions contend with are largely due to testing approaches and requirements that can be dramatically improved via the adoption of advanced auditing technology and approaches.

Fulfilling the massive potential of next-generation internal audit requires recognition that this transformation consists of more than a collection of discrete activities. Becoming a next-generation internal audit function requires a commitment to continual evolution, particularly in healthcare provider organizations.

Richard Williams, Protiviti's Global Healthcare Leader, suggests, "It is becoming more critically important than ever before for internal audit functions to serve as a mission-critical strategic business partner to the organizations they serve. Internal audit plans and special project assistance should be developed and executed in a manner that aligns to organizational priorities and ensures the results could become integral to the successful pursuit of an organization's mission, innovation and/or ministry."

Top Internal Audit Priorities

In addition to zeroing in on innovation/transformation progress and challenges, this year's study takes a broad look at overall areas of focus for internal audit functions in healthcare organizations, including their top audit plan priorities. Following is a look at several notable priorities identified in our study. Brief commentary for each is provided on the pages that follow.

1. Billing and Collections
2. Vendor/Third-Party and Joint Venture Risk Management
3. Accounting, Finance and Accounts Payable
4. Fraud Risk Management
5. Regulatory Compliance and Ancillary Services
6. Cybersecurity Risk/Threat and Program Effectiveness
7. Charge Capture
8. System Implementations
9. Enterprise Risk Management

Billing and Collections

A confluence of factors necessitates the need for a more agile, data-driven, and proactive internal audit function for healthcare organizations. First is the accelerating pace of technological innovation, such as cutting-edge data-analytics and use of artificial intelligence, employed by both provider organizations and external auditing organizations. Second is the increased necessity to do more with less as profit margins continue to compress for provider organizations. Last is the increased skill and aggressiveness with which governmental and payer auditing organizations (e.g., Office of Inspector General [OIG], Medicare Audit Contractors [MACs], Office for Civil Rights [OCR], payer auditing programs) identify and pursue enforcement actions. Fortunately, when it comes to revenue cycle assessing and monitoring, there are two powerful tools that a next-generation internal audit function can leverage: use of financial data analytics and in-depth coding/medical record reviews.

Internal audit can effectively leverage provider and payer transactional data, such as the Health Insurance Portability and Accountability Act (HIPAA) electronic data interchange (EDI) 835 electronic claim remittance advice and the 837 electronic claim billing transaction data sets, as a beacon for identifying where there may be potential risks and/or process inefficiencies across the revenue cycle. For example, by mapping the American National Standard Institute (ANSI) codes to root cause categories (e.g., medical necessity, coding error, authorization), internal audit can quickly identify key areas of opportunity or noncompliant practices that result in payer denials. One area where a high number of claims are commonly denied pertains to ANSI code CO16 – Missing Documentation Non-Medical. This code

indicates that key documents (e.g., consent forms, appropriate signatures) necessary for processing a claim were not provided or were not completed properly. Another example of a denial code that often indicates process improvement opportunities is a high volume of CO15 – Authorization denials. This code indicates that the process of obtaining payer authorization is not effective and should be comprehensively assessed. These data analyses point the internal audit function to areas where further investigation of various revenue cycle processes may be needed for ensuring timely and compliant billing to payers.

A coding/medical record review can also provide valuable information surrounding both documented patient care and the effectiveness of revenue cycle processes. If internal audit identifies an increasing or high volume of denials due to Coding or Medical Necessity, it may make sense to perform a coding/medical record review of denied accounts to determine whether the coding was accurate and founded on the provider documentation, and whether the provider documentation fully demonstrated the need for the level of care provided (e.g., inpatient versus observation). Medical records contain a wealth of information concerning both the patient care and revenue cycle functions, such as Patient Access, Case Management, Clinical Documentation Improvement programs, Discharge Planning and so on. For example, a review of accounts in which patients left Against Medical Advice (AMA) may indicate a problem with patients not fully understanding their financial obligations, problems effectively discharging patients, or problems with communication among the provider team and the patient and/or their family members. These examples often indicate the need for a more in-depth review of various revenue cycle functions and provide internal audit with valuable information for developing their audit plans.

Often, internal audit identifies multiple process opportunities that suggest the need to perform a more comprehensive review of the revenue cycle, especially the billing, collections and denials management processes. Given the extensive interconnectedness of each function within the revenue cycle, attempting to understand and rectify process weaknesses or deficiencies within one component often reveals additional process opportunities in other areas or functions of the revenue cycle. This is one of the key reasons so many organizations elect to perform a comprehensive revenue cycle assessment to determine the organization's overall financial health and to mitigate future risks and inefficiencies that may negatively impact net revenues.

Vendor/Third-Party and Joint Venture Risk Management

Vendor management is an area that many healthcare organizations continue to struggle with. The need to focus on effectively managing vendors that support critical business functions or care delivery solutions continues to grow and expand. The industry has seen an explosion in the quantity of vendors providing outsourced or specialty services, back-office solutions, technologies, etc. Healthcare providers use third-party vendors to find the best approach to deliver optimal care and service to their patients but may not understand the risk these vendors pose to their organization's finances and reputation (e.g., security, privacy) — and potentially to patient safety. Additionally, given increasing regulatory scrutiny, it is critical that appropriate contract language is agreed upon and business associate agreements (BAAs), which protect the organization, are obtained when necessary. Even where healthcare organizations have a well-

established vendor-intake process, performing ongoing vendor reviews is often insufficient to address continuous changes to the business, which introduces additional risks to the entity. There are many risks, but perhaps the most pressing risk that needs continual evaluation is data security, which includes the protection of patient data. Internal audit can add value to the vendor management function by assessing the process the organization takes to classify and perform due diligence on vendors based upon inherent risk, as well as how contractual documents are being created, retained and reviewed as a function of that identified risk. Further, internal audit should evaluate the vendor risk management life cycle to determine how effectively the organization is utilizing ongoing assessment and performance monitoring mechanisms (e.g., scorecards, questionnaires, on-site assessments) to manage the overall portfolio of vendor risk.

Accounting, Finance and Accounts Payable

Historically, many healthcare internal audit functions have focused on "patient centric" audits that impact either patient experience, billing and collections, or security and privacy. The results and impact of these audits can be quickly felt throughout the organization. A small percentage of the audit budget is actually spent evaluating the "financial health" of an organization. To date, many of the accounting and finance functions in healthcare organizations are behind the times with updating their finance technology such as enterprise resource planning (ERP), workflow, optical character recognition, electronic data interchange, and consolidation and reporting tools. Additionally, new accounting standards such as revenue recognition and lease accounting are increasing the burden on the accounting and finance teams to do more without additional resources. As organizations are evolving and growing (either organically or through acquisition), the finance and accounting back office is finding it difficult to scale and provide the same or improved services in areas such as payroll, accounts payable and financial reporting as in years past.

Auditors of today's healthcare organizations must take into consideration this evolution and partner with their finance and accounting teams to move their capabilities forward. Next-generation audits can utilize the vast amounts of data that currently reside in the organization's ERP system to identify process inefficiencies and bottlenecks. Additionally, healthcare boards and audit committees, including those of nonprofit organizations, are eager to strengthen controls and continually protect the assets of the organization from fraud and misuse to the point of developing Sarbanes-Oxley type programs even when one is not required by a regulatory body. Automated controls and continuous/automated testing of those controls are paramount to the creation of a high-functioning internal audit function.

Fraud Risk Management

Fraud, waste and abuse are an unpleasant reality in today's healthcare environment. As a result, executive leadership is increasingly interested in fraud risk management to help protect the bottom line. Understanding healthcare organizational vulnerabilities and establishing an appropriate framework to identify and respond to them are essential in today's environment, as regulators are increasingly demanding more active management and investigation for a wide range of risks, including financial crime, fraud and corruption.

Leadership is often in denial about the loss of significant revenue due to fraud. Leaders tend to remain focused on the company's year over year growth and delivering shareholder value while not taking into account how potential fraud may be affecting that bottom line. On the other hand, regulators and prosecutors are holding corporate executives and directors accountable, not only for acts of fraud or bribery they themselves may have committed, but also for similar acts by the organization's employees that they did not take clear action to prevent. This is underscored by a recent Supreme Court of Delaware decision, ruling that a corporate board breached its fiduciary duties (*Marchand v. Barnhill, et al.*).[3]

Fraud prevention is the baseline of fraud risk management and has traditionally consisted of simple controls designed to set an ethical and moral tone and limit the opportunity for fraud. Such measures are a good start, but they need to be part of a comprehensive and ongoing fraud risk management strategy that includes third-party due diligence, fraud auditing, brainstorming sessions and data analytics. One of the most common anti-fraud controls is a high-functioning, well-established and integrated next-generation internal audit function.

Regulatory Compliance and Ancillary Services

Healthcare providers operate in one of the most highly regulated industries in the United States and across the globe. With the increase in scrutiny and enforcement, coupled with the complexity and pace of legislative and regulatory change, compliance continues to be a primary concern for providers. Therefore, it is no surprise that compliance is a key area of focus for internal audit. In addition to billing compliance (including coding and documentation integrity), which was already discussed, the other top compliance areas that we consistently see as part of an internal audit plan are (1) assessing the effectiveness of an organization's compliance program, (2) HIPAA, and (3) drug diversion and the opioid crisis.

On April 30, 2019, the U.S. Department of Justice's (DOJ) Criminal Division published enhanced guidance for the evaluation of corporate compliance programs. This guidance requires prosecutors to attempt to evaluate the effectiveness of an organization's compliance program following a determination of a firm's noncompliance. The prosecutor's opinion as to the effectiveness of the compliance program can impact a range of outcomes, including the decision to file charges, plea agreements and sentencing

[3] For more about this decision, *see Board Perspectives: Risk Oversight*, Issue 118, "The Caremark Standard: Tough, but Not Impregnable," 2019, Protiviti: www.protiviti.com/US-en/insights/bpro118.

recommendations. It is important to note, however, that this guidance does not replace or diminish multiple compliance program guidance publications of the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS), which will likely remain the core standards used should an organization's program be evaluated. The DOJ guidance asks a few new questions for compliance program evaluators to attempt to answer and reinforces many elements with which healthcare industry compliance professionals should already be familiar. The DOJ's framework poses three "fundamental questions" on which prosecutors should reach a conclusion:

1. Is the corporation's compliance program well-designed?
2. Is the program being applied earnestly and in good faith?
3. Does the corporation's compliance program work in practice?

As internal audit functions assess the effectiveness of their healthcare organization's compliance function, it is important not only to use the OIG compliance program guidance and the enhanced DOJ guidance as the framework for the review, but also any other compliance program effectiveness requirements. For example, take into consideration the Medicare and Medicaid Program's Reform of Requirements for Long-Term Care Facilities Rules, which outline the compliance program requirements for long-term care facilities. There are currently proposed changes to the rules.

HIPAA continues to be a major focus for providers with penalties that have surpassed the $100 million mark for HIPAA violations. Clearly, the data protection movement is in full force, and organizations will need to increase their resources to meet the demand of complying with regulations and to prevent penalties as well as reputational damage. Internal audit functions have been placing a heavy emphasis on the effectiveness of security risk analyses, breach risk assessment processes and business associate agreements. Given the use of social media in this digital age, healthcare providers struggle to address associated privacy implications, which should be another focus area for internal audit functions.

Moreover, the opioid crisis is still making headlines every day, and we are starting to see momentum in how health systems are responding to the needs of their patients and communities. Utilizing data analytics to monitor prescribing practices and compliance with opioid initiatives (e.g., prescription drug monitoring programs [PDMP] compliance, pain management contracts) and implementing predictive analytics to drive change are key priorities of hospitals and provider groups across the country. Maturing opioid stewardship committees are developing and implementing process changes beyond the pain clinics to advance education to providers and patients and increase referrals for proven treatments of substance use disorders (SUD). Of course, assessing controls to prevent and monitor for drug diversion is still top of mind for hospital executives, and the ability to use data analytics to focus monitoring efforts has improved efficiency and effectiveness of those reviews. We continue to see redevelopment of drug diversion programs and enhanced security features to ensure proper controls within the supply chain and during the administration and waste processes.

Cybersecurity Risk/Threat and Program Effectiveness

Today's healthcare organizations have a strategic focus to increase adoption of technology to move toward a more connected delivery model. These new technologies, coupled with a diverse and complex business structure and a heavily regulated environment, create a challenging but necessary focus on information security. Criminal cyber attacks utilizing ransomware, phishing, malware and other nefarious exploits are some of the most impactful issues affecting the healthcare industry. The reality for many organizations is that lives could be at stake. Internal audit functions should be playing a key role in helping monitor the effectiveness and adequacy of the cybersecurity program. Internal audit has a unique opportunity to help organizations understand how strategic efforts have an impact on cyber risk and can be managed without being a barrier to innovation. Internal audit needs to embrace the critical role of being a partner in the organization's cybersecurity program. That partnership should span providing assurance around the full spectrum of cybersecurity capabilities, including foundational compliance (e.g., security risk analyses, HIPAA), operating effectiveness of controls and programs (e.g., penetration testing, removal of terminated employees' access, governance of data interfaces, user access to sensitive data repositories like the data warehouse), and the ability to respond once events do occur (e.g., incident response readiness, disaster recovery plans and testing). Healthcare provider boards, audit committees and senior leaders want to know if their cyber programs are effective. This includes maturity and performance of the cybersecurity program, sufficient allocation of resources dedicated to cybersecurity efforts, optimal procedures utilized when cybersecurity incidents occur, and cybersecurity leaders (e.g., chief information officers and chief information security officers) who bring credibility and influence. Internal audit clearly can provide meaningful insight in these cybersecurity domains to their board, audit committees and senior leadership teams.

Charge Capture

It is vital for today's healthcare providers to maximize the revenue received for the services they provide. Ineffective internal controls for key revenue cycle processes can affect net revenue by as much as 3 to 5%, but focused attention to revenue cycle functions typically will enhance revenues and margins through improved strategy, processes and system controls. The charge capture, charge description master, charge posting and charge validation processes are critical elements of the overall provider revenue cycle. Unreliable and/or inconsistent charge capture and reconciliation controls, poor documentation of services and supplies provided and coded, and missed charges can have a significant negative impact on a healthcare organization's overall revenue. The next-generation internal auditor considers ways to employ data analytics for identifying missed charges or charging errors along with performing coding/medical records reviews to identify charge capture process improvement opportunities and documentation and coding improvement activities that lead to optimized reimbursement and an increased overall revenue.

System Implementations

Organizations that are selecting, implementing or managing large-scale systems such as electronic health records (EHRs) or ERP solutions face a significant challenge in identifying, measuring and managing the unique risks they face. Such efforts often go awry when people, process, and technology risks are not given adequate consideration. These risks, when not managed properly, translate to missed opportunities to transform and improve processes, operations and patient care. Although every large-scale system implementation is unique, the risks inherent in these programs are largely consistent across all programs. The internal audit function can help significantly reduce these risks by playing a role that is educational, consultative, or audit in nature, and by bringing deep independent subject-matter expertise to the most common risk areas. Internal audit's ability to operate across the enterprise and across all individual work streams in a program provides visibility to risks that might otherwise be lost between silos. Internal audit can, and should, have a role in these efforts across:

- Business process readiness and solution design
- Program management and governance
- Data conversion and governance
- Organizational change enablement
- Testing strategy
- Reporting and analytics
- Security and internal controls
- IT and business operational readiness

Business continuity and disaster recovery is also an important aspect associated with system implementations. In today's environment of rapid digital change, growing cyber concerns and outages impacting the healthcare industry, effective business continuity and disaster recovery continues to be top of mind. This is magnified by healthcare's increasing reliance on technology and the large-scale system implementation efforts referenced above. Given the heavily regulated nature of the industry, healthcare organizations have long focused on effective emergency preparedness programs to ensure the continuity of care during a disruption. However, many administrative and back-office functions continue to struggle with effective business resumption practices and at times can be left languishing during extended disruptions. Internal audit can play a key role in assessing the effectiveness, both from a design and ongoing operational effectiveness perspective, of overarching programs related to business continuity and disaster recovery. In doing so, an enterprisewide focus should be placed on the full spectrum of crisis management and communications, business resumption planning, and IT disaster recovery. Ineffective risk management during system implementations increases the potential for system outages and extensive downtime, all of which can have far-reaching implications for healthcare providers and patient safety.

Enterprise Risk Management

Due to the vast, rapid and complex changes happening across the industry, it is becoming increasingly difficult for organizations to manage risks proactively and capitalize on potential opportunities. Therefore, organizations are renewing their focus on enterprise risk management (ERM) methodologies to evaluate, prioritize and address risks that could prevent the company from reaching its desired goals, missions and strategic objectives. Admittedly, the healthcare industry is behind the curve when it comes to understanding and embracing the fundamentals of true ERM. Those organizations that can proactively anticipate, adapt and respond to change will be successful. Many organizations are looking to internal audit's expertise in identifying and evaluating risks to help facilitate the ERM journey. With the recent release of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM – Integrating with Strategy and Performance Framework, a new emphasis has been placed on integrating risk with decision-making. Whether organizations have robust ERM programs in place or haven't even started, the updated framework serves as a solid foundation as either a sounding board for current efforts or to help provide direction for future efforts. The updated framework emphasizes the importance of the interconnection of risk, strategy and enterprise performance.

There is no cookie-cutter approach to implementing ERM, and in reality, no two organizations typically take the same approach. However, at its core, four themes are critical to effective integration of ERM, and they are further specified in the framework as follows: (1) strategy-setting and execution has to work in tandem with the organization's defined risk appetite, (2) risk reporting cannot be performed as an isolated exercise and should be integrated with performance measures, (3) a strong foundation with risk governance and culture should ensure that pressures within the organization are not incenting unintended consequences, and (4) risk considerations should be tied into decision-making processes.

An effective ERM system provides management with relevant information regarding risks, uncertainties and opportunities that could influence decision-making during strategy- and objectives-setting and performance management. In that respect, ERM needs to evolve from a "risk listing" to a "risk informed" decision-making approach. A risk-informed approach to ERM is an important differentiator that proactively supports an organization's chances of success in achieving its strategic objectives and performance goals.

In Closing

Clearly, internal auditors within healthcare provider organizations have their hands full. Regulatory compliance requirements, along with other unique, healthcare-specific risks, tend to make their audit plan priority lists longer and more complex than those in other industries. While these unique challenges may, to some extent, explain why internal audit innovation and transformation within healthcare providers lag other industries in key technology and methodology areas, audit leaders should resist letting their teams mentally accept that excuse.

Instead, chief audit executives should bear in mind that becoming a next-generation internal audit function requires an innovative mindset and culture that encourages reexamining the foundational elements of the internal audit function's capabilities, charting a transformational course, and then executing those plans while concurrently having team members perform their day jobs. Change is hard. Change requires courage. But change is necessary for internal audit to be a true partner and adviser to boards, audit committees and senior leaders. Ultimately, in order to succeed, next-generation efforts require an internal audit culture that embraces change, because without question, the rest of the organization is changing.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 75 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contact

Richard Williams
Global Healthcare Practice Leader
+1.469.374.2469
richard.williams@protiviti.com

protiviti®
Face the Future with Confidence