BARNES & THORNBURG LLP

2025 Healthcare Compliance Outlook

Emerging Cybersecurity, Data and Regulatory Risk in the Age of AI

Executive Summary

Compliance is a critical line of defense for healthcare organizations as they navigate complex regulations, mounting cyberattacks and rapid-fire technological change. Yet the majority of U.S. compliance professionals surveyed in Barnes & Thornburg's inaugural Healthcare Compliance Outlook report are stretched thin and feeling less than confident as new risks – including those associated with the explosive growth of artificial intelligence (AI) – add to their workload. That concern may be warranted: our research identifies several missed opportunities that could deepen healthcare organizations' exposure to risk.

Barnes & Thornburg surveyed 120 compliance, risk and legal leaders across U.S.-based healthcare and life sciences organizations, including hospital systems, physicians' practices, and pharmaceutical, biotech and medical device manufacturers.

Respondents included CEOs, chief compliance officers, chief risk officers and in-house counsel, all of whom either lead or support compliance and risk matters within their organizations. Organizations ranged in size from entities with less than $1 million in annual revenue to those generating $1 billion to more than $10 billion each year.

Our research looked at the hurdles facing healthcare compliance professionals in the year ahead and examined how their organizations are addressing high-risk areas. We also explored how the industry is currently using AI for internal legal compliance functions and what steps organizations are taking to ensure proper governance and oversight.

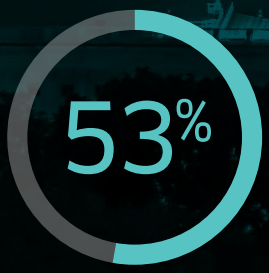
More than half of respondents report resource constraints in compliance program areas like budget, staffing and technology, all while costs continue to grow as healthcare organizations incorporate AI into their operations. These stresses could potentially affect care delivery: only 42% are very confident when it comes to maintaining high quality of care in light of compliance and risk issues. Significantly, in this constrained fiscal environment, more than half (54%) of respondents say their organizations have either accepted, are seeking or are considering private equity (PE) backing. And more than a quarter (27%) of those who aren't currently considering PE backing say they would do so in the future, highlighting the increased importance of private capital.

Our AI findings were revealing, underscoring that health risk and compliance professionals – like those in other industries – are setting up AI-related policies in a relative vacuum as the use of tools like generative AI outpaces the development of regulatory frameworks. Beyond compliance reports, there is no consensus among organizations that have already implemented AI on other measures to guide its ethical use. Despite that, nearly three-quarters of respondents are either already leveraging AI in their internal legal compliance functions or are considering it, with organizations embracing both predictive and generative AI for data analysis, risk assessments, administrative tasks and other uses.

With these and other compliance pressures looming, such as proliferating data privacy requirements, our overall findings suggest organizations may not be using all the tools at their disposal. Just 48% of respondents say their organizations currently audit high-risk areas and even fewer collaborate with external industry, legal or compliance partners or regulatory bodies as part of their compliance and risk-mitigation strategies. Considering all of this, it's not surprising that less than one in three say they are "very prepared" to meet future compliance and risk challenges.

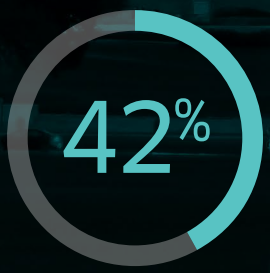
Overall, we found that while healthcare risk professionals are aware of the hazards around AI integration, data privacy and other compliance hotspots, organizations could be doing more to proactively safeguard their businesses and support patient health. In what follows, we'll explore those findings in greater detail and offer guidance to help healthcare risk, compliance and legal leaders adapt to this dynamic regulatory environment against a backdrop of mounting risk and limited resources.

Key Findings
Compliance

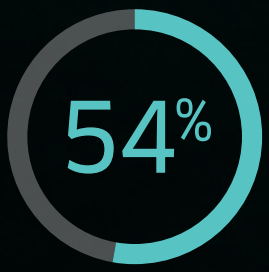


More than half (53%) of healthcare compliance and risk leaders report resource constraints in program areas like budget, staffing and technology; **56%** predict forthcoming limitations

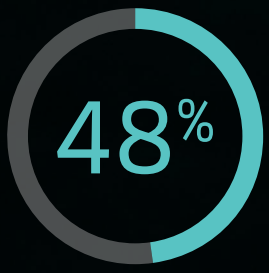
Only 31% feel "very prepared" to meet future compliance and risk challenges



Less than half (42%) are "very confident" about maintaining high quality of care in light of compliance and risk issues



More than half (54%) of organizations are already seeking PE backing or considering it



Less than half (48%) audit high-risk areas, and even fewer currently collaborate with external industry, legal or compliance partners or proactively engage with regulators as part of their compliance and risk mitigation

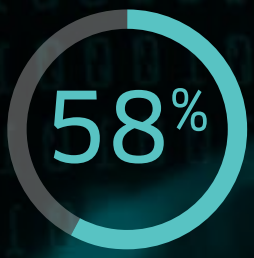
Key Findings

AI

Nearly 3/4 of respondents are using or considering using AI – both generative and predictive – in their internal legal compliance function; data analysis, risk assessments and administrative tasks are the most popular applications

>10%

Six in 10 of those respondents say that AI integration and development will add **more than 10%** to their budget in the coming year



58% of all respondents say developing a governance structure for AI compliance is difficult. Beyond compliance reports, there is no consensus among organizations that have already implemented AI on what measure to guide its ethical use

Compliance and Risk Landscape

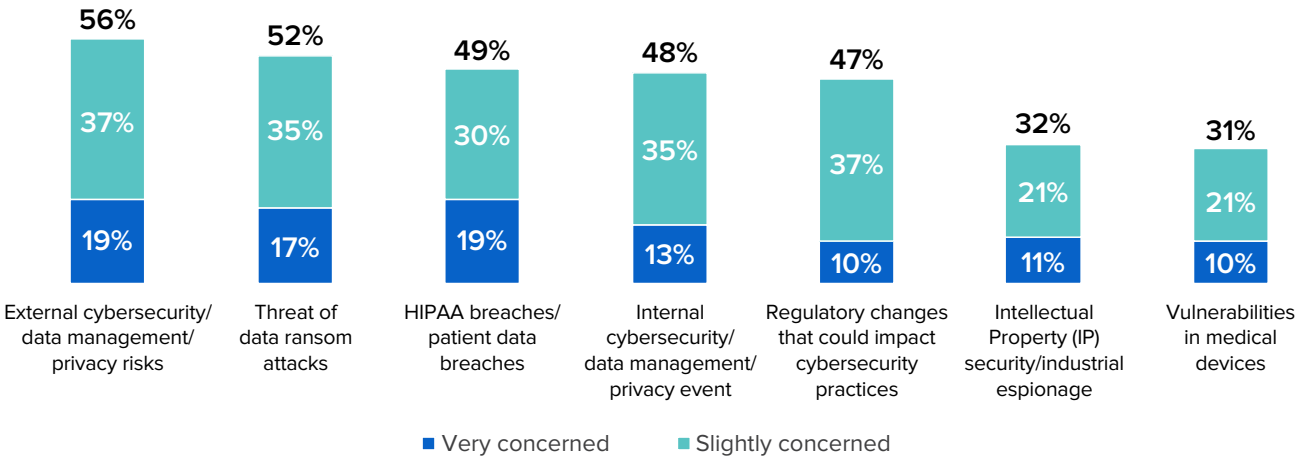
From costly ransomware attacks to evolving guidance around cybersecurity under the Health Insurance Portability and Accountability Act (HIPAA), the healthcare industry is confronting mounting risk and compliance responsibilities heading into 2025.

Only 4% of respondents say the current compliance and risk issues facing their organizations do not concern them – and fewer than one in three say they are "very prepared" to meet future compliance and risk challenges. How those challenges evolve could depend, in part, on the 2024 presidential election, given the two candidates' divergent views on regulation. Regardless of the outcome, effective compliance programs will continue to be critical for minimizing corporate risk.

Sufficient defense against cyberattacks is casting a particularly long shadow over the industry amid fallout from recent incidents like the Change Healthcare data breach. Fifty-six percent of respondents cite external cybersecurity/data management/privacy risks as a concern for the coming year, with similarly high levels of concern surfacing around the threat of data ransom attacks (52%) and HIPAA/patient data breaches (49%). Internal cybersecurity/data management/data privacy events and regulatory changes also ranked as key concerns, cited by 48% and 47%, respectively.

Some organizations may be less equipped than others to navigate the above challenges, whether that's due to resource limitations, the size of their internal risk and compliance teams – half (50%) have five or fewer employees on such teams – or the degree to which they collaborate with external industry, legal or compliance partners or proactively engage with regulators.

As it relates to cybersecurity, how would you rate your level of concern regarding the following issues in the upcoming year?



Compliance priorities and pressures

Given these responses, it tracks that security and privacy top the list of priorities for healthcare organizations, selected by two-thirds (66%) of those citing concerns about risk and compliance issues. Auditing high-risk compliance areas (48%) is next, followed by staying up to date with emerging federal/state regulations (45%) amid a raft of privacy, quality and safety requirements that affect everything from provider referrals (e.g., the Stark Law and Anti-Kickback Statute) to telehealth and how organizations bill for and code medical procedures, conduct laboratory tests, and store and distribute controlled substances.

Enhancing/updating compliance documents and frameworks is also a concern (39%). As for organizations that are conducting audits, they are most focused on data privacy and security (63%), with a much lower share doing them for areas such as fraud, waste and abuse prevention (26%) or patient privacy (22%).

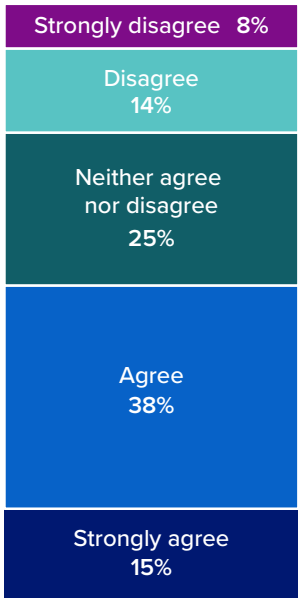
Which of the following issues represent current priorities for your organization? (Select all that apply)

** Question was asked to those who indicated the current compliance and risk issues facing their organization are at least somewhat concerning*

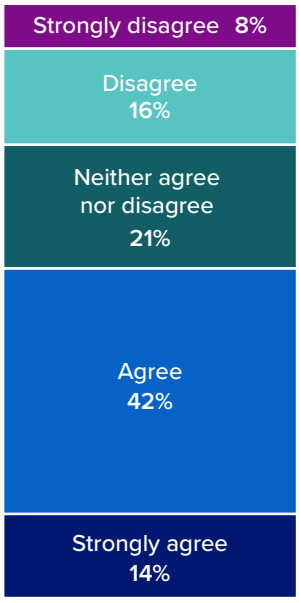
Notably, less than half of respondents with compliance and risk concerns see such audits as a priority, which ties back to another theme in our research: the constraints facing healthcare risk and compliance programs. The majority (53%) of survey respondents say they are experiencing resource limitations in their compliance programs, and 56% expect to encounter them over the next year. Budgetary pressure is the leading limitation, with five in 10 of the above groups citing constraints on financial resources, followed by those relating to skilled talent and technological resources (44% and 38%, respectively).

Organizations anticipate more trouble ahead on this front in the coming year, with staffing issues/talent shortage ranking as the top concern (50%), followed by financial constraints (46%). As a result, 32% of respondents say addressing these resource limitations and staffing challenges is a priority.

Please indicate your level of agreement to the following statements:

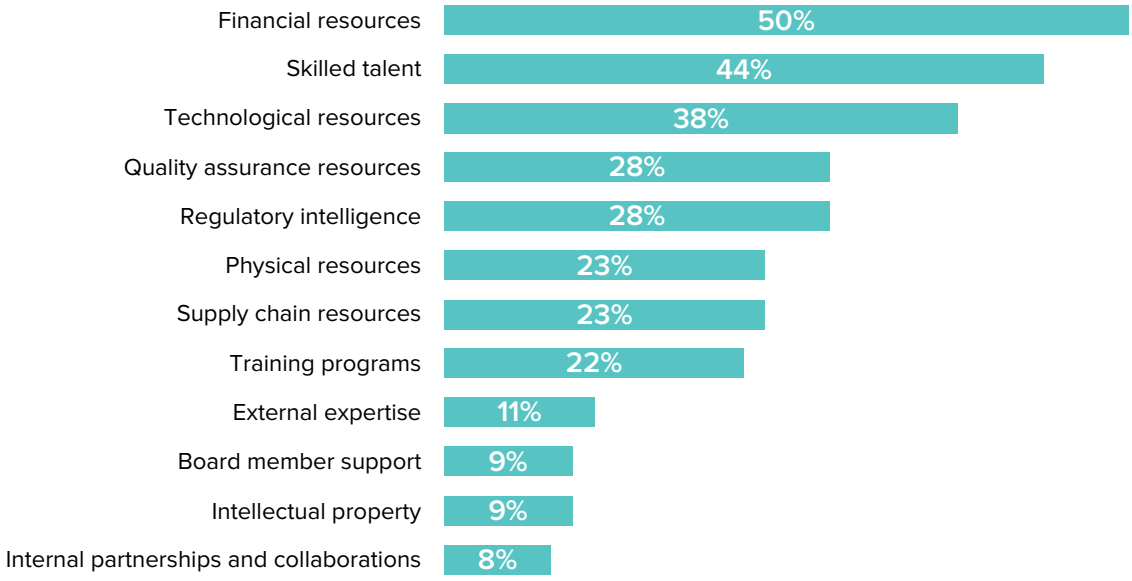


We are currently experiencing resource limitations within our compliance program.



We expect to experience resource limitations within our compliance program over the next year.

Which of the following limitations are you experiencing or do you expect to experience over the next year?



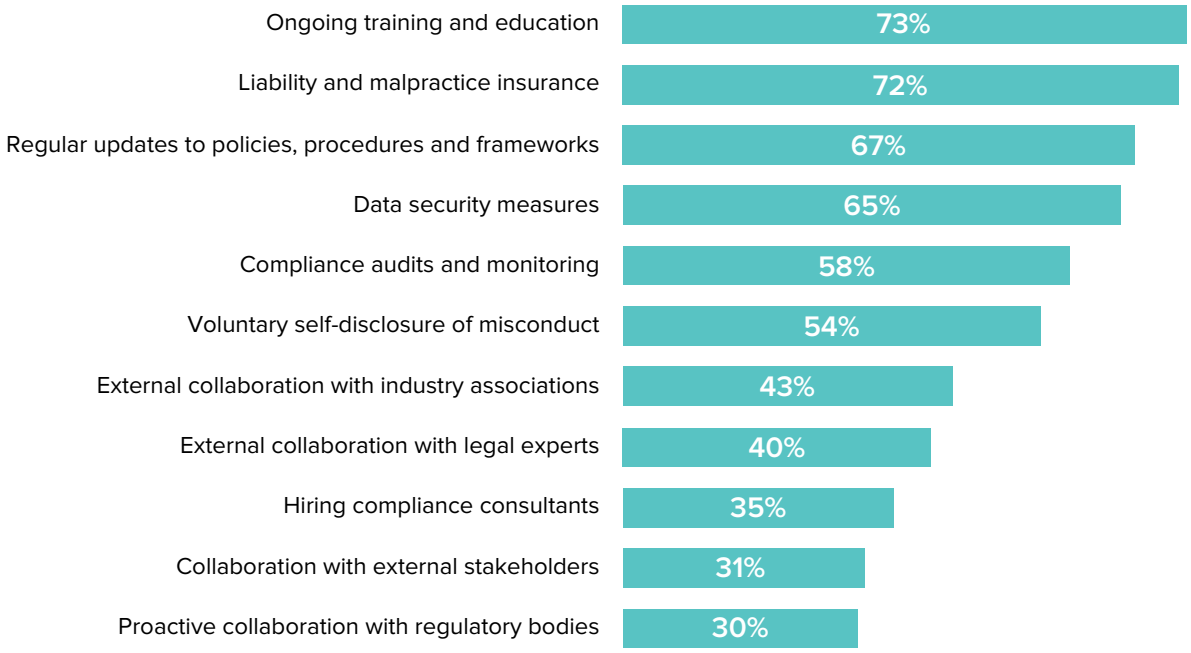
** Question was asked to those who expressed agreement that their programs are currently facing or will face resource limitations over the next year*

Teaming up to mitigate risk

One strategy that could help resource-strapped leaders offset these constraints is teaming up with internal or external groups beyond their own departments to buttress compliance efforts. However, less than half (44%) of respondents are currently doing so, and one-third have not considered such partnerships to date. While roughly one in four healthcare organizations we surveyed collaborates externally with industry associations (43%) or legal experts (40%), only 35% are hiring compliance consultants – and just 30% are proactively working with regulatory bodies.

The industry could be missing out on a vital source of support by failing to embrace cross-functional teamwork and external collaborations. And the stakes are high. We asked respondents how confident their organizations are, in light of their compliance and risk priorities, in maintaining high quality of care – a key issue for the industry. Less than half (42%) said they are "very confident."

Which of the following actions have been implemented or considered by your organization as compliance and risk mitigation tactics?

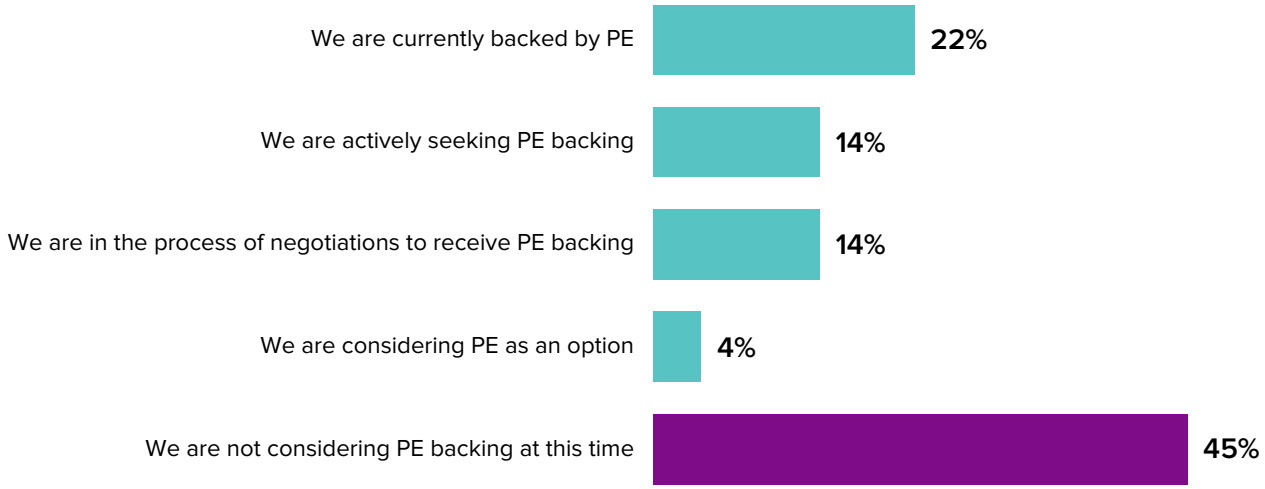


Partnering with private equity

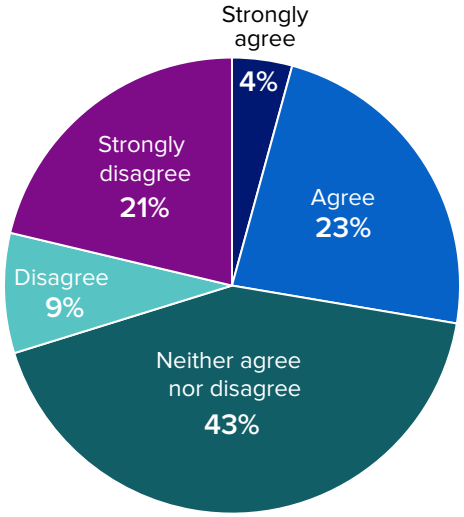
Amid these headwinds, it's perhaps not surprising that the industry is looking to additional sources of capital for support. The healthcare sector is drawing interest from PE due to the aging population and increased rate of chronic diseases; as innovation in drugs and devices advances, so does the need for funding to improve efficiency and services. More than half of respondents (54%) say their organizations have either accepted PE backing (22%), are actively seeking it (14%), are in the process of negotiating to receive it (14%), or are considering it as an option (4%). More than a quarter (27%) of those who aren't currently considering PE backing say they would do so in the future, highlighting the increased importance of private capital in the current healthcare landscape.

To be sure, PE involvement in healthcare has drawn increased scrutiny in recent months as antitrust and other federal and state regulators examine how consolidation influences the quality of and access to care, patient health and medical workers. Healthcare PE deals must navigate a complex landscape of federal and state regulations beyond antitrust – including the Anti-Kickback Statute, self-referral prohibitions and the corporate practice of medicine doctrines – and ensuring compliance is critical to avoid legal, financial and reputational risks. However, such "buy-and-build" strategies can offer significant benefits for organizations, and a number of deals have moved forward despite challenges.

Which of the following represents your organization's status when it comes to receiving backing from private equity (PE)



Please state your level of agreement to the following statement: Although we are not considering PE backing at this time, we would do so in the future



** Question was asked to those who expressed that their organization is not considering PE backing at this time*

Compliance and risk guidance

Cyberattacks

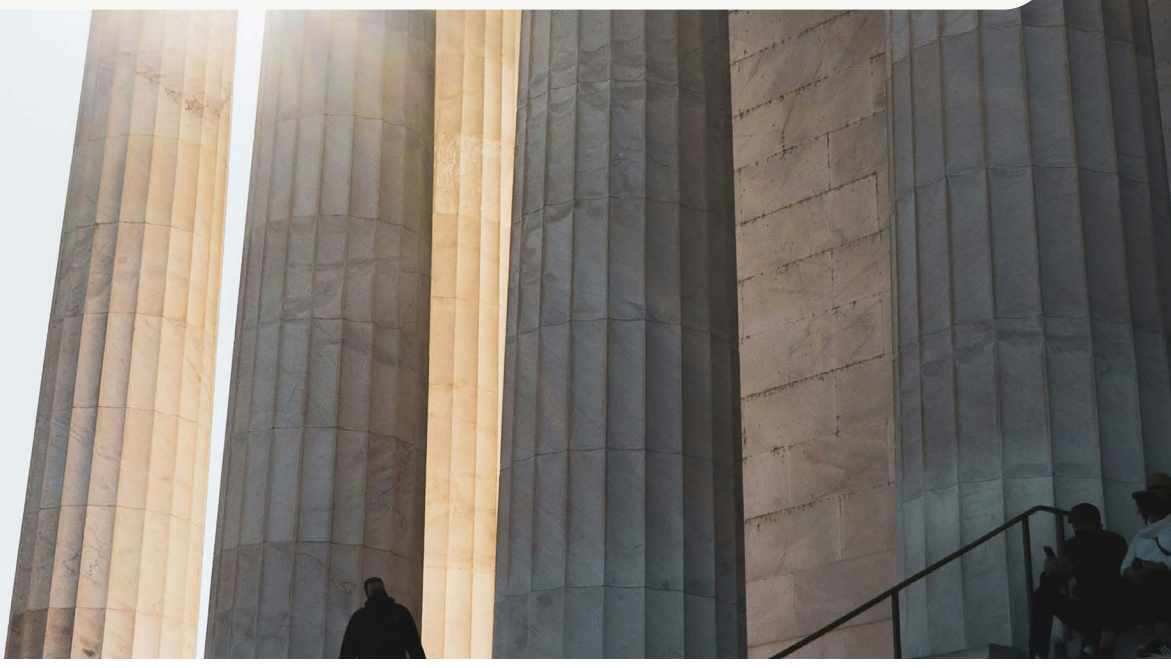
Unfortunately, we expect that ransomware and phishing attacks will only increase in the coming year, so it's critical to be prepared on all fronts. Companies should consider continued investment in effective threat-detection tools, including AI-powered ones. To comply with evolving federal and state requirements, organizations should employ strong incident response plans and conduct regular simulations and employee training.

Compliance priorities

Healthcare organizations should consider implementing continuous monitoring systems and controls to keep pace with rapidly changing regulations. It's important to conduct proactive internal audits to identify risks and address potential compliance gaps.

Private Equity

As PE investment in healthcare accelerates, organizations considering such opportunities should anticipate increased scrutiny and oversight at the state and federal levels. Organizations considering a PE-backed deal should ensure they conduct thorough due diligence and comply with complex regulatory and enforcement requirements.



AI Implementation and Ethical Use

Like the rest of the business world, the healthcare industry is ablaze with AI fever; like businesses across the spectrum, the healthcare industry must weigh the potential advantages against concerns around accuracy, data privacy and more. Current conversations touch on everything from HIPAA and third-party vendor contracts to whether to build or buy AI-assisted technology – plus what proper oversight and governance look like as organizations proceed with AI investments.

Our research shows that multiple C-suite roles may take the lead in such matters, with the CEO front and center (56%). Interestingly, while half of the organizations we surveyed report their compliance teams include a chief compliance officer, only one in three said the chief compliance officer takes a leading role in AI matters. This mixed picture may be due in part to the current dynamics around generative AI, where companies see the nascent technology as a business imperative but are also wary of the associated risks. CEOs may be leading on generative AI while compliance and risk-oriented C-suite roles oversee predictive AI, which is more mature.

Generative and predictive AI in healthcare compliance

Generative AI

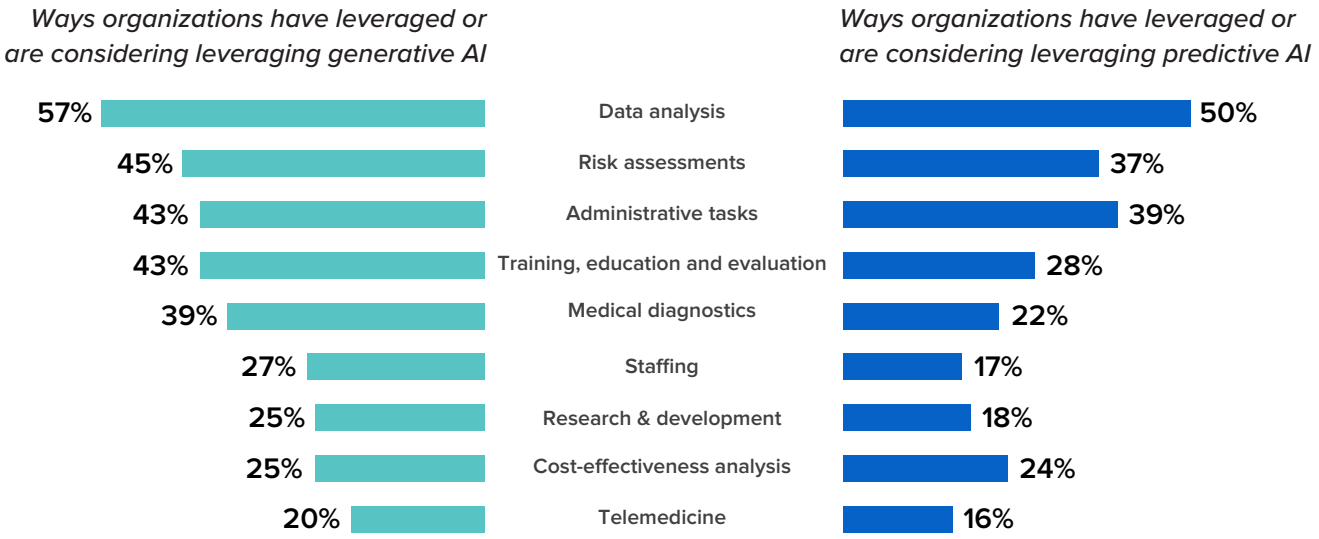
Generates new content, such as images, text or music, based on patterns learned from existing data (e.g., training content/policy generation, scenario simulation, system testing).

Predictive AI

Utilizes machine learning and historical data to forecast future outcomes or trends (e.g., risk assessments, fraud and anomaly detection).

Nearly three-fourths of respondents say their organizations are either using or considering using AI – both generative and predictive – in their internal legal compliance functions. Generative AI has a slight edge, with 31% having already implemented it, compared to 28% for predictive AI, which is more specialized and less easily applied to basic tasks.

Data analysis, risk assessments and administrative tasks are the top ways organizations are leveraging or considering leveraging both generative and predictive AI. The former appears to have deeper penetration across multiple tasks, potentially because of the relative ease of launching or customizing generative AI solutions – essentially, using ChatGPT for various functions – via application programming interfaces (APIs).



With that said, the jury is still out on how generative AI can be used for internal legal compliance functions. Predictive AI has the longer track record, including in the regulatory risk assessments that are central to many compliance teams' work. Of respondents who are using it for that function, 40% say predictive AI is "effective" and 17% rate it "very effective."

As for where they're sourcing these tools, 41% of respondents are commissioning a solution from external sources, with a surprisingly robust 36% choosing to develop them in-house. One-third are buying a preexisting AI solution, and 32% are adapting a proprietary version derived from publicly available technology – which means organizations need to rigorously evaluate the risks and terms attached to those tools, such as who owns the data entered into these systems and how these tools are trained.

However, those paths diverge to some degree depending on the type of AI, with a slightly higher percentage of predictive AI implementers opting to outsource compared to generative AI (57% versus 52%); conversely, fewer predictive AI implementers are adapting publicly available technology (30% versus 36%).

Governance and oversight

With potential applications for AI multiplying even as regulatory frameworks are still being devised, compliance and risk leaders acknowledge the challenges ahead. Fifty-eight percent of respondents say that developing a governance structure for AI compliance in their organization is difficult at present, with 52% anticipating some degree of difficulty over the next 12 months.

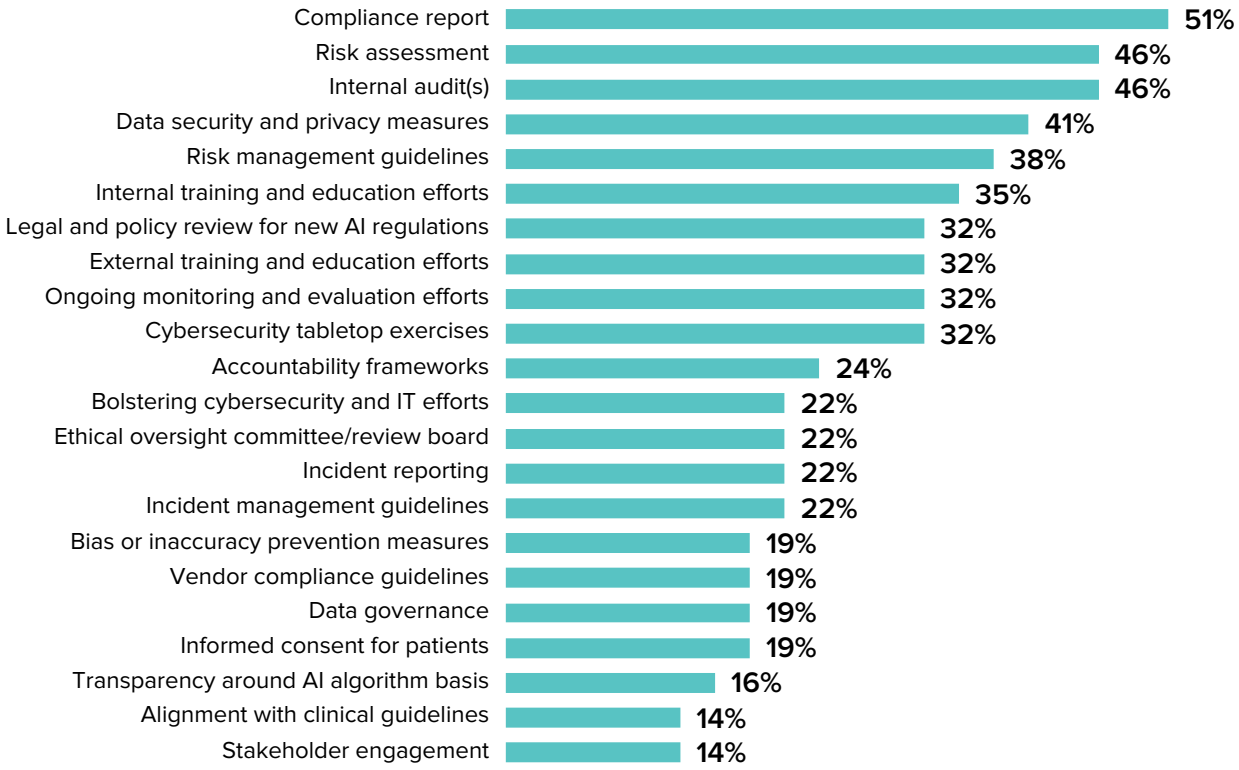
Asked what measures are most important to maintain ethical standards around AI use, the majority of respondents (53%) said frequent risk assessments. These assessments far outpace other options, including ongoing monitoring and evaluation (37%) and internal training and education efforts (34%). Some organizations are also conducting legal and policy reviews for new AI regulations on a monthly basis.

Some healthcare organizations may not have much in the way of AI guardrails at all. This may be in part because there are few regulations yet that would push organizations to create them – another area where developments over the next year could depend to some degree on the 2024 election results. But while compliance efforts are often reactive, all risk, compliance, and legal professionals using AI in their organizations must be proactive. That means setting up policies, guardrails, and procedures and guidelines for use, despite the largely nascent state of AI-specific regulation.

Our findings suggest that when it comes to AI, industry professionals are essentially operating in silos, with little visibility into how peers are approaching the technology. Outside of compliance reports – which 51% of respondents cite – there seems to be no consensus among organizations that have already implemented AI on other measures to guide its ethical use. Though many use risk assessments or internal audits (46%), data security and privacy measures (41%) and risk management guidelines (38%), the general lack of concrete policy is somewhat surprising.

Perhaps this is due to the emergent stage of AI at many healthcare organizations, with some likely more in exploration mode as opposed to leveraging the technology in a meaningful way.

You indicated that your organization is currently leveraging AI in its functions. What compliance measures does your organization have in place to ensure the ethical use of AI? (Select all that apply)



** Question was asked to those who have already implemented generative AI and/or predictive AI*

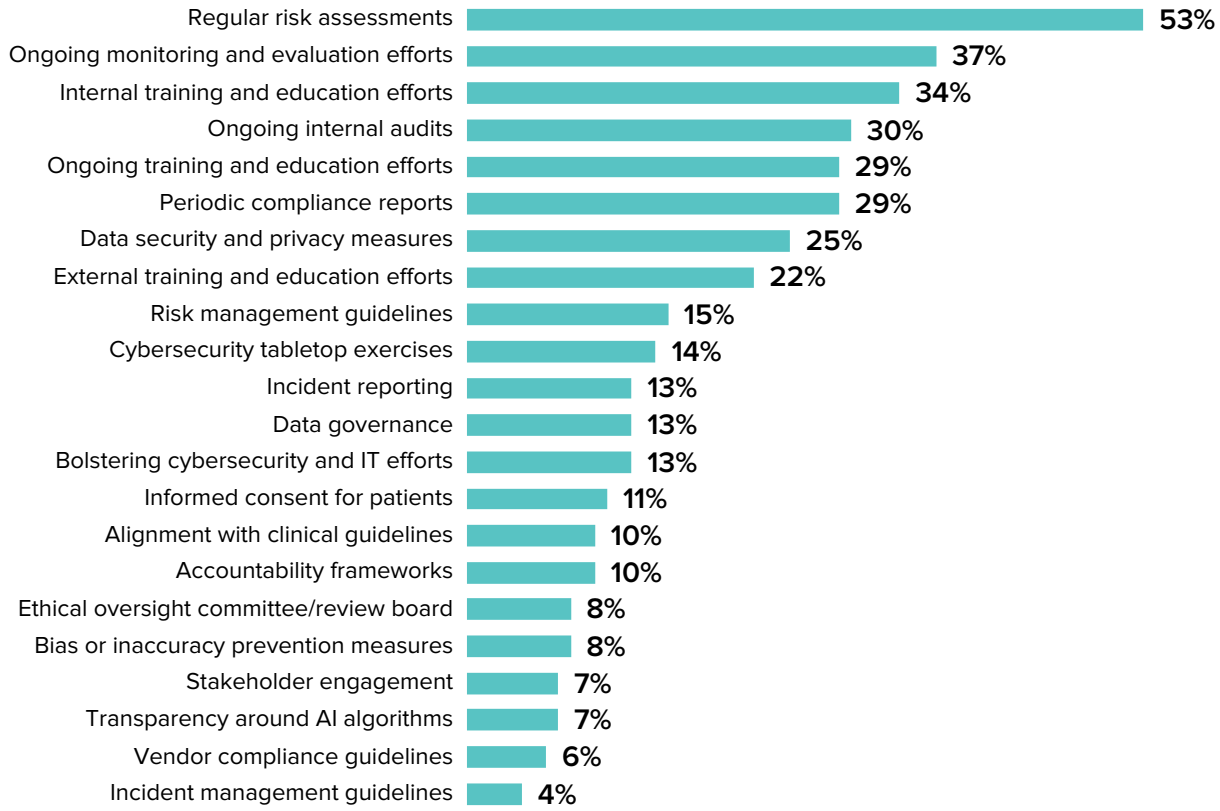
Top AI challenges and costs

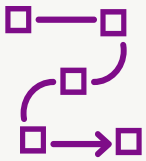
AI-related pressures on healthcare compliance extend beyond governance issues and the hunt for suitable applications. Respondents say the top challenges for AI implementation are data privacy issues (33%), compliance adherence (29%) and data breaches (26%) – consistent with the challenges for risk and compliance programs as a whole.

AI could also have real implications for the bottom line. Of those organizations that are either implementing it or considering doing so, six in 10 expect their budgets for AI integration and development will increase by more than 10% in the next year – and one-fifth anticipate a more than 30% jump. That range could reflect the somewhat haphazard approach many companies are taking with AI; setting out AI-related line items may be less common than simply tallying up expenses that occur during real-time experimentation and trying to account for them after the fact.

Regardless, those anticipated costs come at a pivotal time for healthcare risk and compliance leaders who are being asked to do more with less, even as their remit broadens. Given those constraints, it's critical that professionals use all the tools at their disposal – including using cross-functional teams and proactive collaboration with outside resources – to keep pace.

What measures do you believe are most important to maintain ethical standards around AI use? (Select all that apply)





Plan before you act

Organizations need to have governance policies in place before they launch AI tools, paying particular attention to data privacy and security safeguards as AI technologies penetrate deeper into risk assessment and compliance monitoring. Healthcare companies must review AI tools before they experiment with them to ensure they understand the rules for use and any limitations that such platforms may place on outputs, including whether commercial use to develop new products and services is permitted.

Governance

As AI regulations continue to take shape across jurisdictions, organizations should implement robust frameworks that align with emerging regulatory standards, such as the EU AI Act, and with established AI ethical principles. Healthcare companies should also consider participation in industry initiatives to share best practices.

Challenges and costs

The rapid pace of AI-related change means that legal and regulatory regimes will often be a step behind as new tools and capabilities proliferate. Organizations must prepare for increased compliance costs tied to emerging regulatory requirements like third-party audits, with the expectation that additional expenses will arise as the technology advances.

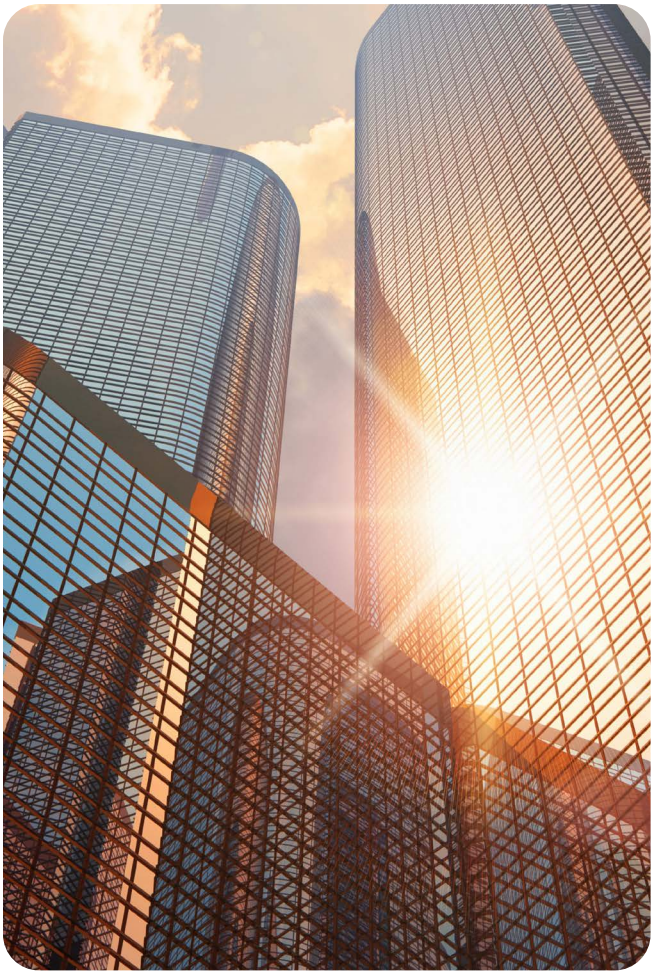
Methodology and Demographics

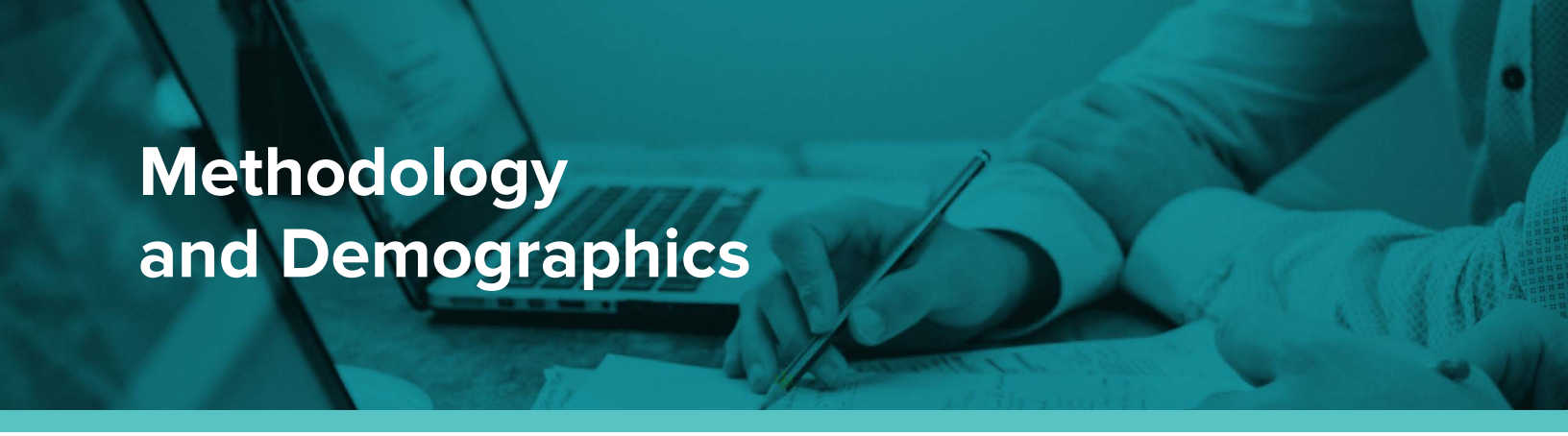
Barnes & Thornburg surveyed 120 compliance and risk leaders with the help of Dynata, a third-party B2B panel provider. The online survey was conducted in May 2024.

The respondents included CEOs, chief compliance officers, chief risk officers and in-house counsel, all of whom played a leading or supporting role in their organizations' risk and compliance matters. Organizational types included hospital systems, physicians' practices, and pharmaceutical, biotech and medical device manufacturers, all based in the U.S.

Organizational size and gross revenues also varied, with nearly half of the respondents reporting annual revenue above $10 million, and 10% above $1 billion.

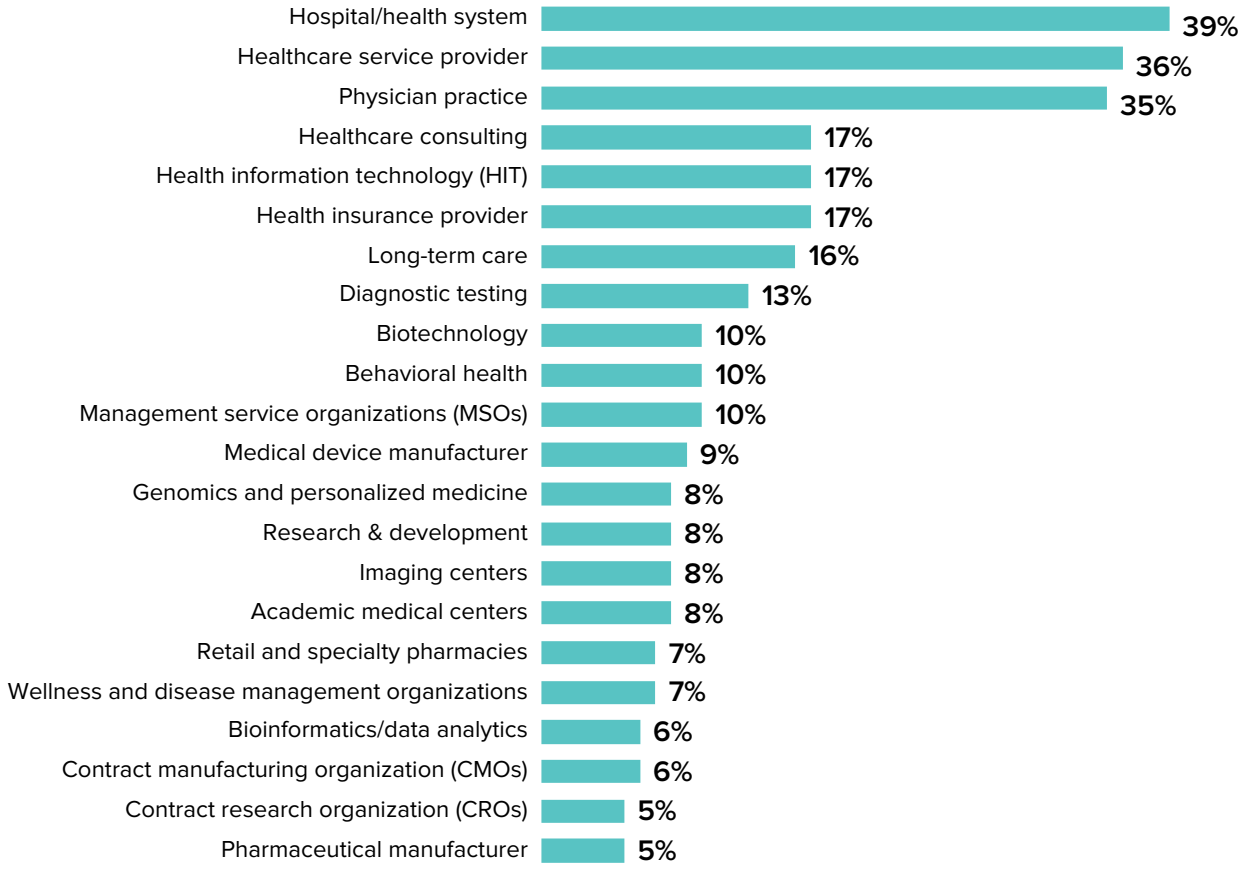
Responses were anonymous and data was analyzed in the aggregate. Due to rounding and questions to which more than one response was allowed, data may not add up to 100%.



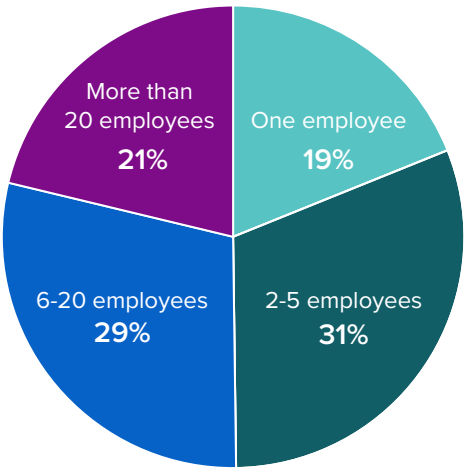


Methodology and Demographics

Additional focus areas



Size of compliance and risk management team



About Barnes & Thornburg

Healthcare Industry Practice and Data Security and Privacy Practice

Barnes & Thornburg stands out because of our deep healthcare and life sciences industry knowledge, paired with our practical and innovative advice. With more than 100 healthcare industry practice attorneys in the firm, located across the country, we offer clients access to unmatched experience and subject-matter expertise. Many of our healthcare industry practice attorneys have worked for federal and state regulatory and enforcement agencies, healthcare and life sciences companies, and hospital/health systems. This allows us to understand the unique challenges of our clients and provide valuable guidance through the maze of complex statutes, shifting regulations, and compliance program needs on matters involving Medicare and Medicaid, internal and government investigations, complex litigation (including commercial, criminal, and civil FCA litigation), data privacy and healthcare technology requirements, managed care contracting, payor disputes, audits and reimbursement, operational and regulatory questions, mergers and acquisitions, and other legal and compliance issues facing all sectors of the healthcare industry. We provide trusted guidance to your varied needs while minimizing risk and meeting business objectives.

Barnes & Thornburg's data security and privacy attorneys help companies analyze and mitigate risks related to the collection, storage, use and distribution of data. We work to help clients establish risk management policies, business continuity procedures, and data breach responses. By putting together effective contractual provisions with vendors and comprehensive cyber insurance policies with insurance providers, we help companies better manage and, where appropriate, transfer the risk of cyberattacks and data breaches. We keep abreast of the constantly changing federal and state laws and regulations governing specific industries as well as businesses in general.

But more than just dealing with the legal risks of data breaches, our attorneys also help clients cope with the public relations and reputation management aspects of cyberattacks. From our wide-ranging work in regulatory, technology, healthcare, insurance coverage and security issues for some of the largest companies in the world, our attorneys identify data security and privacy issues and advise clients on ways to improve their procedures and business positions.

Contributors

JOHN E. KELLY
Partner, Barnes & Thornburg
Chair, Healthcare Department and Healthcare Industry Practice

BRIAN J. MCGINNIS
Partner, Barnes & Thornburg
Co-Chair, Data Security and Privacy Practice

BARNES & THORNBURG LLP