



HEALTHCARE AI READINESS INDEX

COTIVITI x MedCityNews



Introduction

Cybersecurity is an underdiscussed topic in the context of artificial intelligence, yet AI could make malware and phishing attacks against hospitals and insurers even more potent — a serious risk given the compelling evidence of the healthcare industry's interest in adopting AI and making it part of their tech infrastructure. Hospitals and health insurers are considering applying AI tools to a variety of burdensome administrative tasks, but since AI tools require larger volumes of data to train algorithms, how are institutions protecting that data? And beyond security, how are healthcare executives thinking about deployment more broadly: what areas have the greatest potential for transformation, and what are the barriers to adoption?

The **2026 Healthcare AI Readiness Index**, a new report by Cotiviti and MedCity News, explores how healthcare leaders are balancing AI's potential with the operational, regulatory and security challenges accompanying its deployment. A survey of 70 executives from payers and providers in the summer of 2026 offers candid perspectives on these issues.

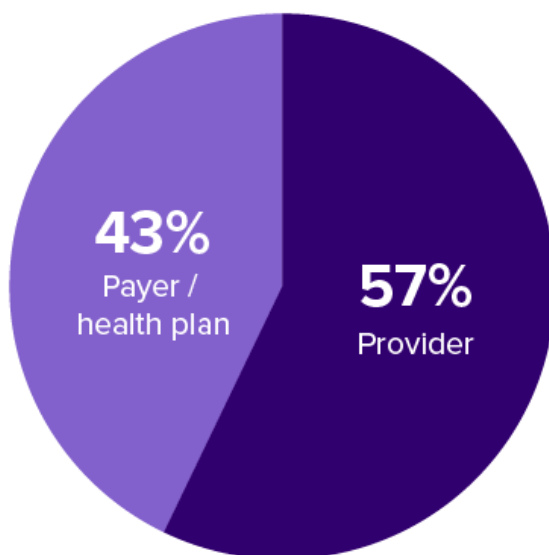
The findings suggest that healthcare organizations are adopting AI faster than they are building the governance and cybersecurity frameworks needed to use it safely. One notable finding from The Index survey is that less than half of payers and only a third of providers feel very prepared to respond to AI-assisted cyberattacks.

The Index offers new insights into healthcare leaders' views on AI and cybersecurity, highlighting the benefits AI tools are bringing to organizations, the measures these organizations are taking to protect their digital infrastructure, and their primary concerns as use of the technology becomes more widespread.

SURVEY DEMOGRAPHICS

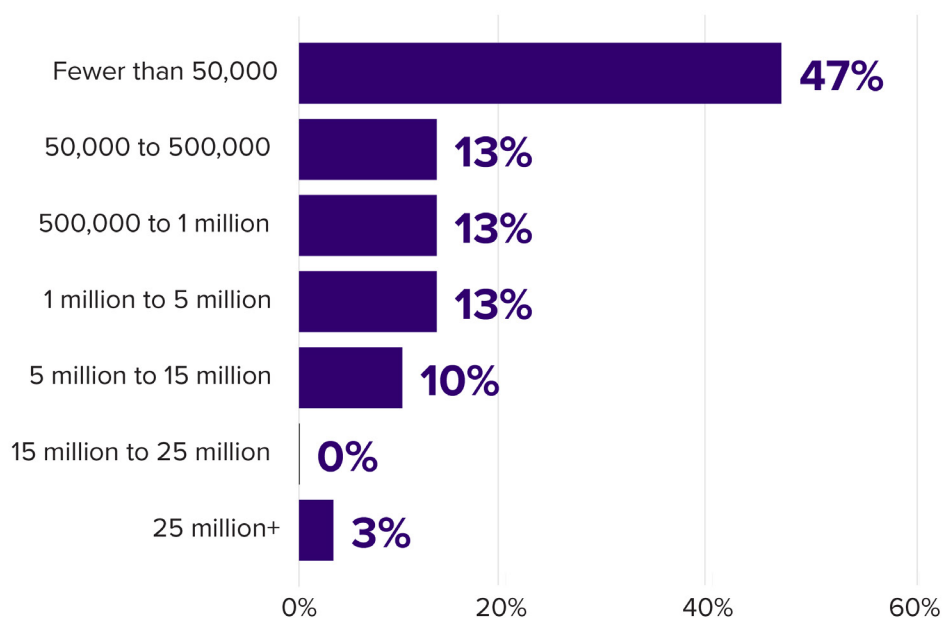
ORGANIZATION

What type of organization do you work for?



PAYER SIZE, BY NUMBER OF MEMBERS

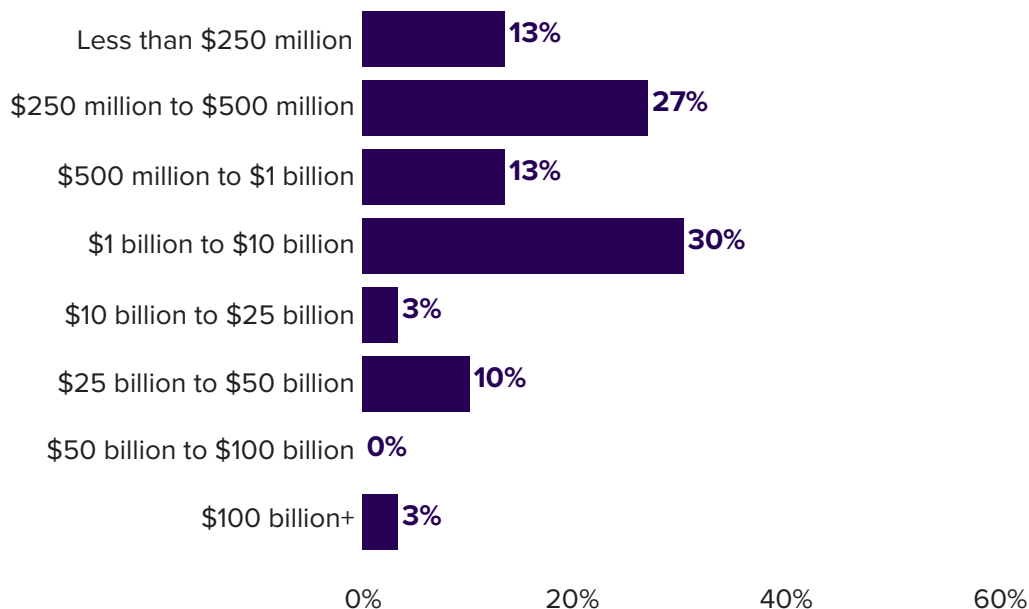
How many members does your organization have?



SURVEY DEMOGRAPHICS

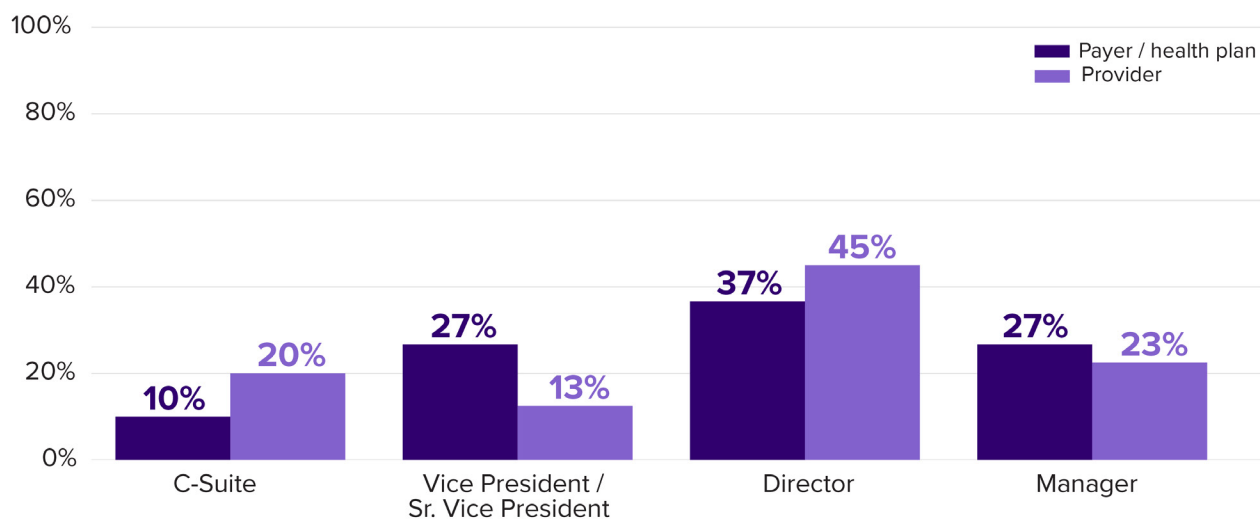
PAYER SIZE, BY REVENUE

Which of the following best describes your organization's revenue?



JOB ROLE

Which of the following best describes your job role?



Key Findings

- 97% of payers and 93% of providers surveyed are either piloting or actively using AI, and almost 40% of health insurers say that it is a core aspect of their business.
- The primary barriers to adoption of AI are regulatory issues and data security concerns.
- The majority of respondents at both payer and provider organizations believe that clinical recommendations and appeals are functions that always require human review, regardless of AI capability.
- For health insurers, the most common metrics for measuring the success of AI include cost savings, improved member satisfaction, and faster claims adjudication.
- For providers, the top metrics are improved patient satisfaction, better clinical outcomes, and cost savings.
- Among payers, the primary benefits of using AI include better member experience, faster claims processing, reduced operational costs and workflow efficiencies, more accurate risk assessments, and improved clinical outcomes.
- Among providers, benefits include reduced administrative workload, enabling doctors to spend more time with patients rather than updating records, accelerated data analysis, and faster information processing.
- While the majority of respondents have some policies to govern employee use of AI, less than 40% have detailed policies in place.
- 60% of payers and 64% of providers report that employees are using “shadow AI” tools that are not authorized or integrated with their IT systems.
- 52% of payers surveyed are “extremely concerned” about the possibility of AI vendors introducing cybersecurity or compliance vulnerabilities into their systems.
- Just 42% of payers and 32% of providers believe their organizations are “very prepared” to respond to AI-assisted cyberattacks.
- To protect against cybersecurity threats, most payer and provider organizations use data encryption, multifactor authentication, cloud infrastructure, and endpoint protection tools.
- More than 90% of payer and provider respondents expect their organizations to increase investments in AI and/or cybersecurity over the next year.

SURVEY RESULTS

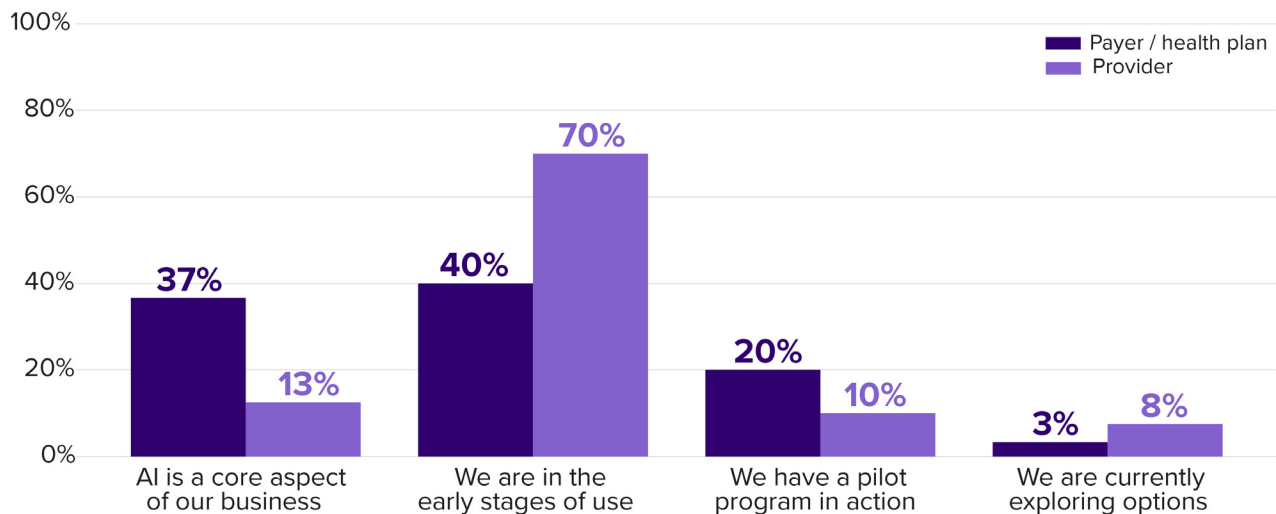
Note that percentages in some charts may not add up to 100% either because of rounding or because respondents could make more than one selection.

Level of Adoption

While not everyone is already implementing AI tools at their organizations, the majority of those surveyed have at least begun using them. Payers are a little further along in the process than providers, with 37% of respondents working in payer organizations describing it as a core aspect of their business. Another 40% said that they are in the early stages of use, and 20% are currently running pilot programs.

Meanwhile, the majority of respondents at provider organizations (70%) said that they are still in the early stages of AI use, and just 13% reported that it is a core aspect of their business.

How would you describe your organization's level of AI adoption?



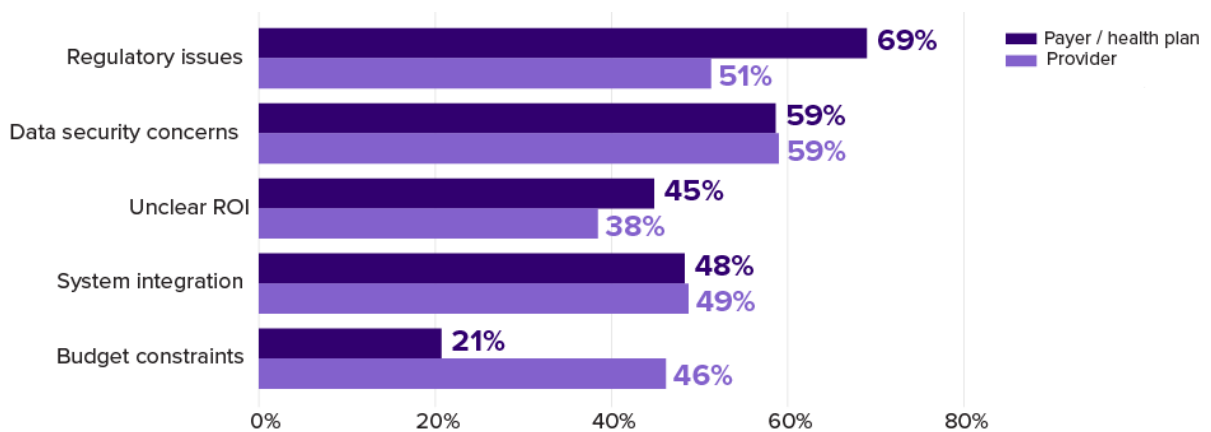
SURVEY RESULTS

The most common barrier to AI adoption among payer organizations is regulatory issues, cited by 69% of respondents. Regulatory issues are also an obstacle for many provider respondents (51%).

Other impediments among both payers and providers include data security concerns (59%) and, to a lesser extent, system integration (48-49%). System integration may be a bigger concern for large organizations: 56% of respondents working at insurers with at least 50,000 members identified system integration as a primary barrier, compared with 38% of those at smaller payer organizations.

Some respondents — 45% of payers and 38% of providers — also said that unclear ROI inhibits the adoption of AI tools at their organization. Budget constraints can also be a factor, though they were cited more often by providers than payers (46% vs 21%).

What are the primary barriers to adoption of AI at your organization?

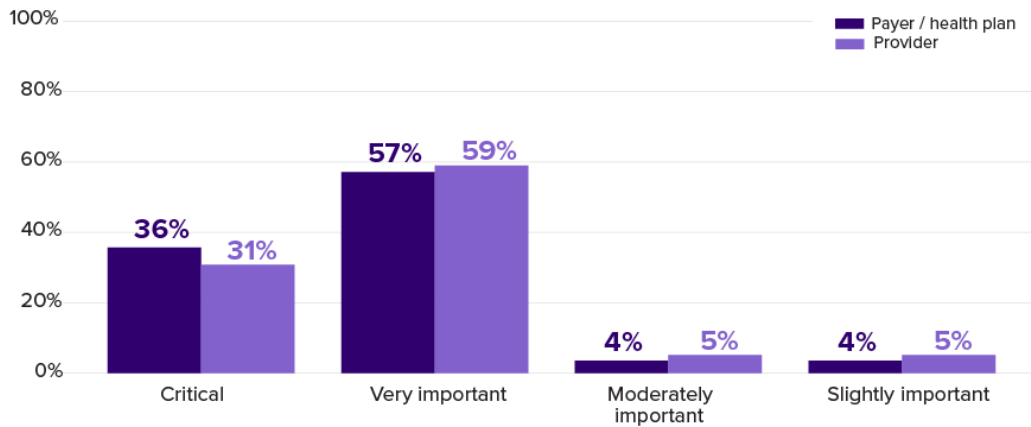


SURVEY RESULTS

Views on Implementation

Nearly all respondents across organizations agree that explainability and transparency in AI-driven payer decisions are very important, with more than 30% saying they are “critical.”

How important is explainability and transparency in AI-driven payer decisions?

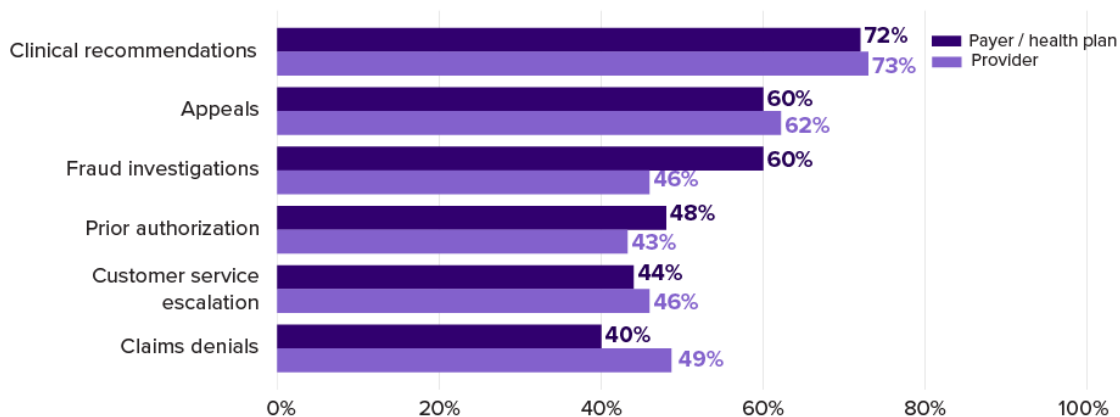


Most respondents also believe that there are certain functions that always require human review, regardless of AI capability — chief among them clinical recommendations, cited by 73% of providers and 72% of health insurers. A majority of both payers and providers also believe that appeals require human review.

There is more divergence of opinion when it comes to fraud investigations, with 60% of payers saying that these require human review, compared with 46% of providers. Payers are also a little more likely to insist on human involvement for prior authorization (48% vs 43%). On the other hand, more providers believe that claims denials require human review (49% of providers, compared with 40% of payers).

Smaller payer organizations may be more willing to leave some functions to AI than larger organizations. For example, 92% of insurers with 50,000 or more members said that clinical recommendations should always involve human review, while just 50% of those with fewer than 50,000 members said the same.

Which functions should always require human review, regardless of AI capability?
Select all that apply.

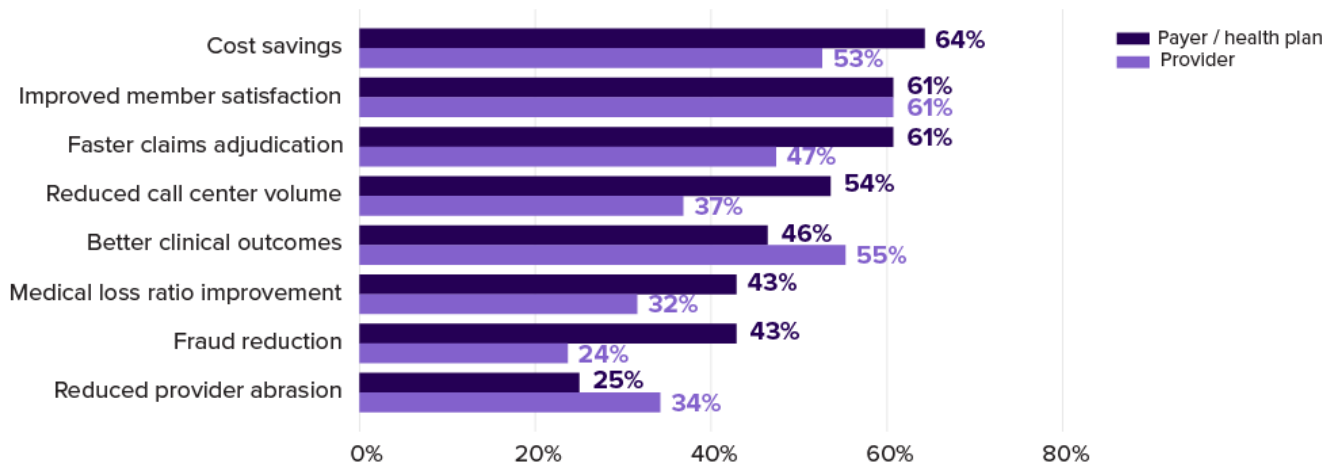


SURVEY RESULTS

Measuring Success

Among health insurers, the most common metrics used to assess the success of AI include cost savings (64%), improved member satisfaction (61%), faster claims adjudication (61%), and reduced call center volume (54%). More than 40% of the payers surveyed also evaluate data on medical loss ratio improvement and fraud reduction. For providers, the top three metrics are improved patient satisfaction (61%), better clinical outcomes (55%), and cost savings (53%).

Which metrics does your organization use to evaluate AI success?
Select all that apply.



What are the primary benefits your organization has seen as a result of using AI tools?

Respondents were asked to share the main benefits their organization has experienced as a result of AI tools. Among the primary benefits cited by payers are better member experience and customer service, in part through the use of chatbots; faster claims processing and identification of billing anomalies; reduced operational costs and workflow efficiencies through automation of tasks; more accurate risk assessments; and improved clinical outcomes.

Some providers note that they are still in the early stages of AI use. Those that are implementing AI appreciate reduced administrative workload, greater efficiency, and increased productivity, resulting in savings of both time and costs. They also note benefits for both clinicians and patients when doctors can spend less time updating records and more quality time with patients, as well as improved care management recommendations. Several respondents also mentioned faster data analysis, allowing for deeper insights to help improve performance.

Sample responses:

Payers / health plans

- “24/7 customer support: Resolves basic inquiries instantly using chatbots”
- “Reduced manual data entry”
- “Faster claims processing”
- “More accurate risk assessment”
- “More personalized member experiences”

Providers

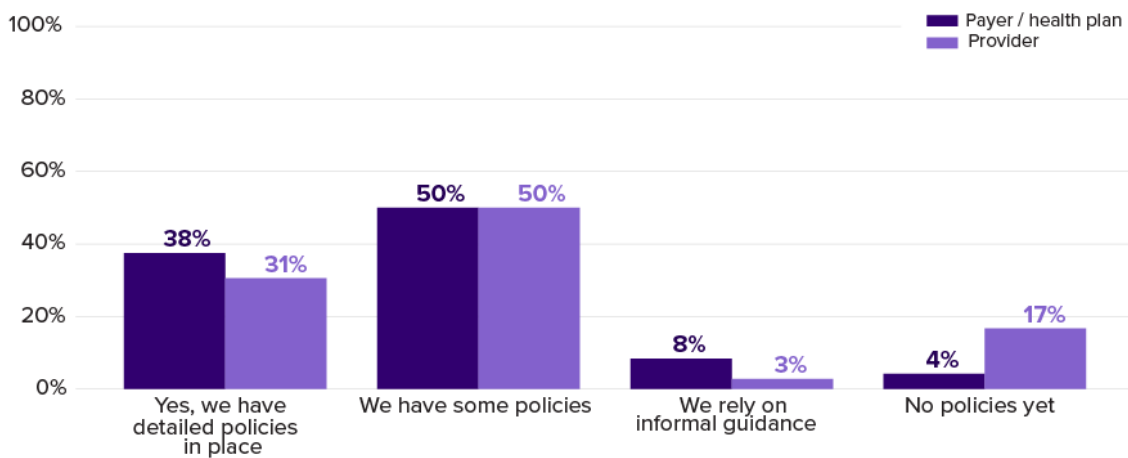
- “Improved compliance monitoring”
- “Better doctor quality of life and timely billing when notes are added to chart on time”
- “We’ve been able to process information much faster. Things that used to take hours now take minutes.”
- “More efficient provider network management.”
- “Just started evaluating it and the primary focus will be on efficiency in low level tasks”

SURVEY RESULTS

Governing Use

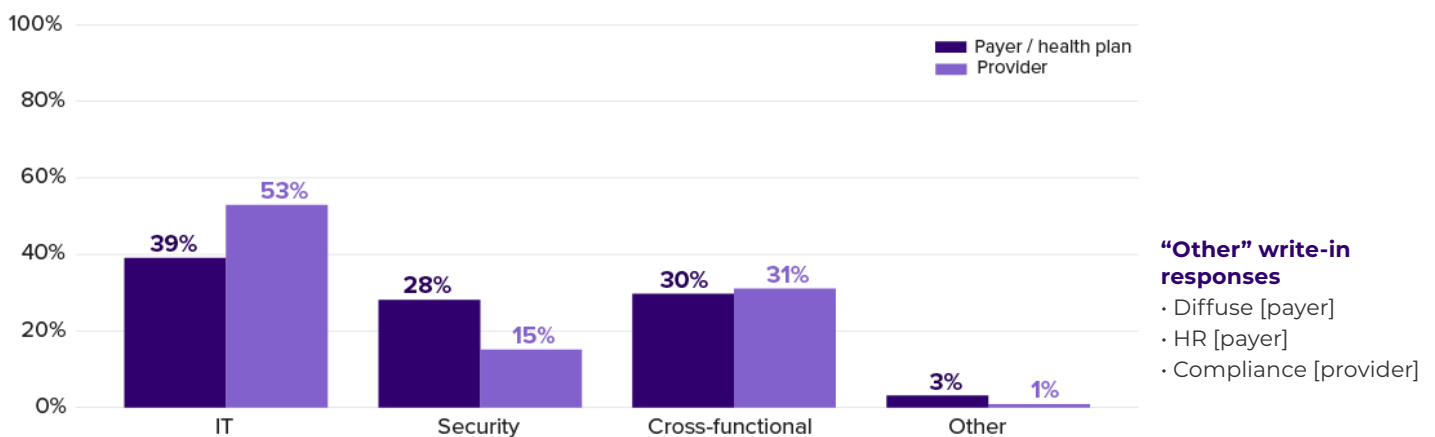
As with the adoption of AI, health insurers are a little further along than providers when it comes to its oversight. More than half of both groups have established at least some use guidelines, but 38% of payers, compared with 31% of providers, have detailed policies in place to govern employee use of generative AI tools. And 17% of providers report that they have not implemented any policies at all.

Has your organization implemented governance policies around employee use of generative AI tools?



While governance of AI use is often handled by the IT department, at some organizations the security team is responsible, and at others it's a cross-functional responsibility.

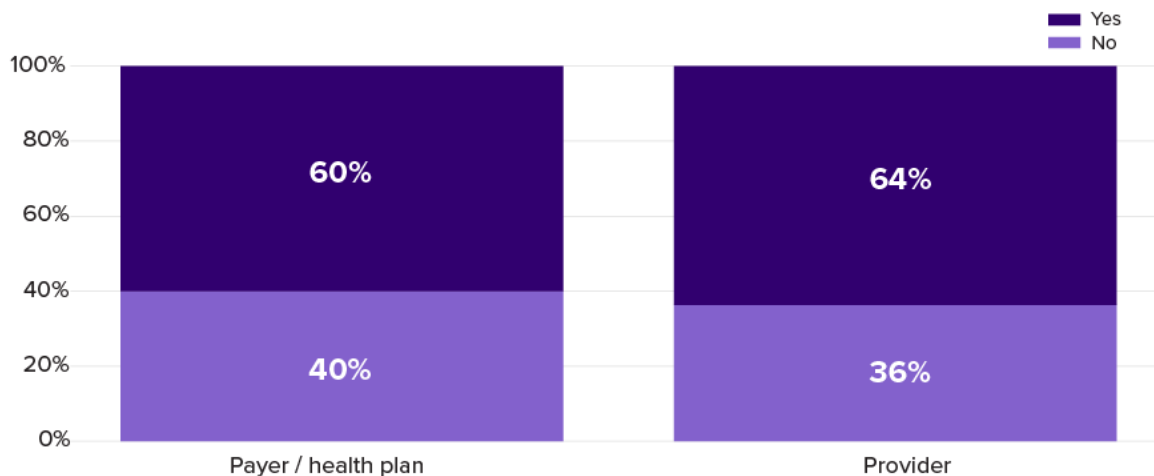
Which department or role is responsible for governance with respect to AI use?



SURVEY RESULTS

The use of “shadow AI” tools is relatively widespread, with 60% of payers and 64% of providers reporting that employees use AI tools that are not authorized or integrated with their IT systems.

Are employees in your organization using “shadow AI” tools that are not officially authorized or integrated with your IT systems?



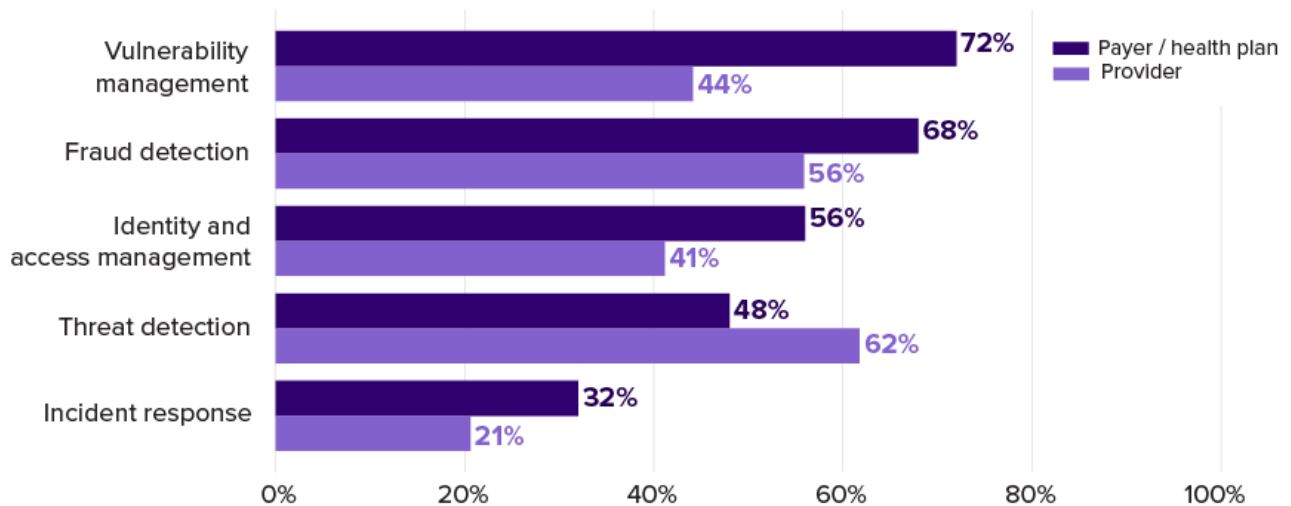
SURVEY RESULTS

Cybersecurity Challenges

The survey results suggest that AI tools may be more widely used for cybersecurity functions at payers than at providers. More than two-thirds of payers said that AI is used for vulnerability management (72%) and fraud detection (68%), and more than half reported that it is also used for identity and access management (56%).

Threat detection is the most common use of AI among providers (62%), followed by fraud detection (56%) and vulnerability management (44%). Forty-one percent of the providers surveyed said that AI tools are used for identity and access management. Relatively few providers (21%) or payers (32%) are using AI for incident response.

Which cybersecurity functions at your company are currently using AI?
Select all that apply.

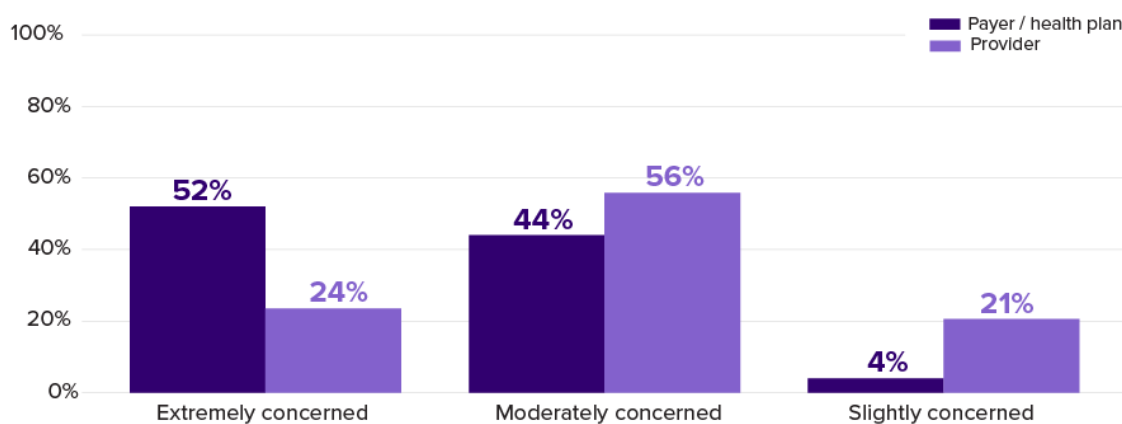


SURVEY RESULTS

Concern about the possibility of AI vendors introducing cybersecurity or compliance vulnerabilities into their systems is especially high among payer organizations. More than half of those surveyed (52%) said they are “extremely concerned” about this risk, and 44% are “moderately concerned.”

Although the majority of providers also have some concerns, most said they are “moderately concerned” (56%) or “slightly concerned” (21%). Just 24% said they are “extremely concerned.”

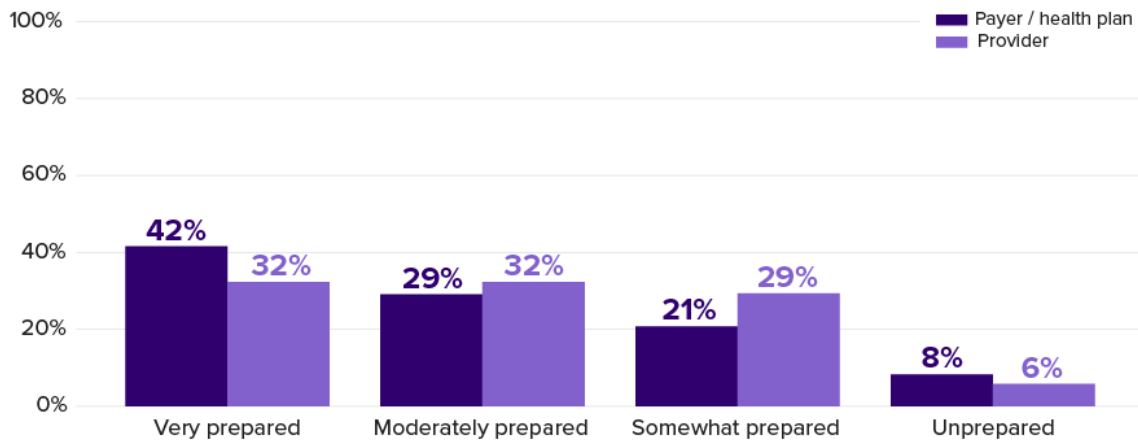
How concerned are you about AI vendors introducing cybersecurity or compliance vulnerabilities?



SURVEY RESULTS

Just as health insurers are a little more concerned than providers about AI vulnerabilities, they are also more likely to be prepared to respond to AI-assisted cyberattacks. Forty-two percent of payers say their organizations are “very prepared” and 29% are “moderately prepared,” compared with 32% of providers who are “very prepared” and 32% who are “moderately prepared.”

How prepared is your organization to respond to AI-assisted cyberattacks?

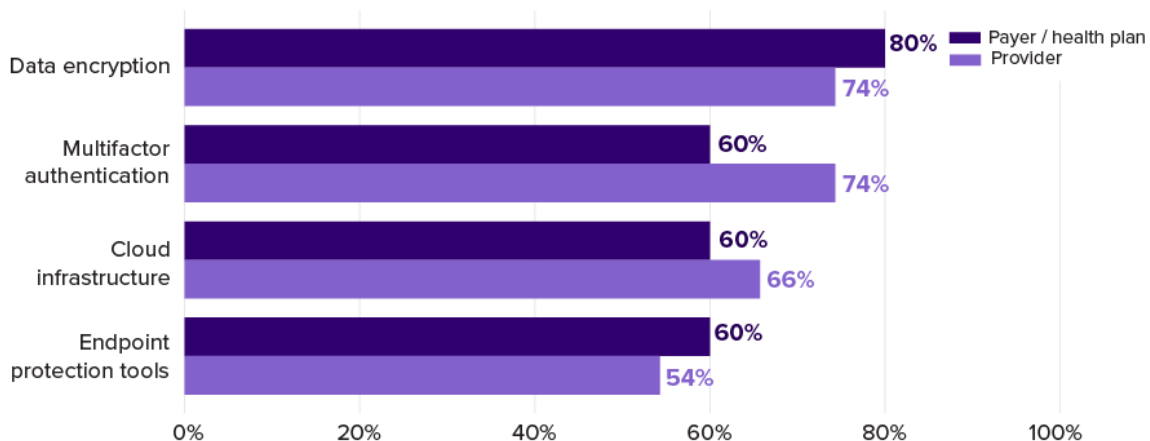


In terms of specific measures to protect against cybersecurity threats, nearly all payers surveyed said their organizations use data encryption (80%) and the majority also use multifactor authentication (60%), cloud infrastructure (60%), and endpoint protection tools (60%).

However, these protections may be more common in large organizations. While more than 80% of respondents at insurers with 50,000 or more members said they use data encryption and endpoint protection tools, among smaller organizations, only 67% use data encryption and 33% use endpoint protection tools. Just 42% of small payers said they use multifactor authentication.

Among providers, most employ data encryption (74%), multifactor authentication (74%), and cloud infrastructure (66%). More than half also use endpoint protection tools (54%).

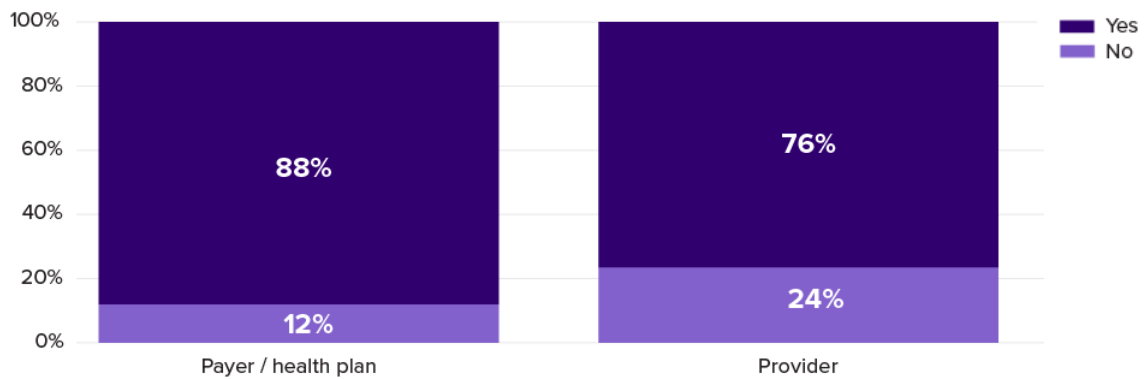
What kind of cybersecurity protections do you have in place? Select all that apply.



SURVEY RESULTS

Most respondents, payers and providers alike, believe that their organization's CISO is involved at the appropriate time during the decision-making process for new technologies, although almost one in four providers (24%) suggested that this is not the case.

Do you feel the Chief Information Security Officer (CISO) is being brought into the decision-making process for new technologies soon enough at your organization?



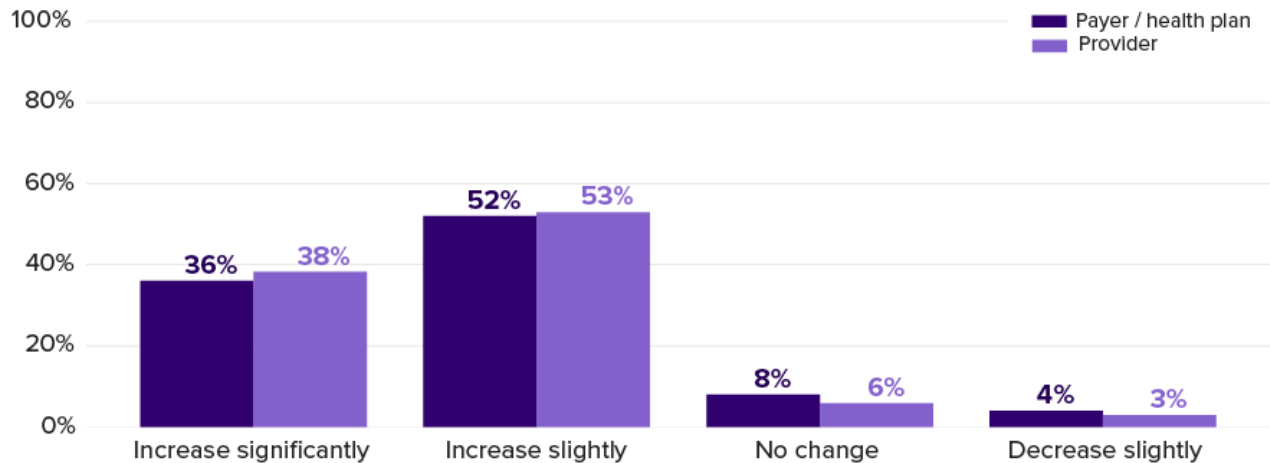
SURVEY RESULTS

What Lies Ahead

The vast majority of respondents expect their organization to increase investments in AI and/or cybersecurity over the next year, with 36% of payers and 38% of providers saying they anticipate these investments to “increase significantly.”

While a small number of respondents don’t expect their organization’s investments to change, very few anticipate a decrease (just 4% of payers and 3% of providers).

How do you anticipate your organization’s investments in AI and/or cybersecurity to change over the next year?



SURVEY RESULTS

Which payer and provider functions are most likely to be transformed by AI within the next 5 years?

Respondents were asked what areas AI is most likely to transform in the next few years. Some of the functions that payers and providers expect to see transformed include eligibility verification, claims processing, prior authorizations, medical coding, and denial management. Respondents also mention referrals to specialists, personalized treatment recommendations, and clinical analysis.

Appointment scheduling and billing are other functions that will likely change. According to one respondent, “RCM as a whole, I think, will be completely taken over by AI eventually.” “I think providers will benefit most from AI documentation tools,” a provider respondent told us. “They can spend less time on paperwork and more time with patients.” A respondent at a payer organization agrees: “It will instantly handle insurance claims, approve doctor requests faster, answer patient questions around the clock, and automatically take notes during doctor visits so physicians can focus on people instead of computer screens.”

Data analysis is another area where respondents foresee transformative developments. AI will provide “deep data mapping of drug efficacies and market pricing to continuously adjust medication tier frameworks” and enable “predictive analytics for disease progression.”

Sample responses:

Payers / health plans

- “Claims, prior authorizations and referrals to specialists”
- “Coding and denial management”
- “Personalized treatment recommendations”
- “Utilization management, claims processing, risk adjustment”
- “It will instantly handle insurance claims, approve doctor requests faster, answer patient questions around the clock, and automatically take notes during doctor visits so physicians can focus on people instead of computer screens.”

Providers

- “Basic functions: approvals/denials, general customer service/question answering”
- “Clinical decision making, payment approvals, scheduling/rostering, resource planning”
- “For patients, better access to their findings; for doctors, easier management of higher-quality medical documentation”
- “Provider network optimization”
- “I think providers will benefit most from AI documentation tools. They can spend less time on paperwork and more time with patients.”

SURVEY RESULTS

What concerns you most about AI adoption in payer and provider organizations when it comes to cybersecurity?

Asked about the impact of AI on cybersecurity, respondents raised a number of concerns — foremost among them, protecting the security of patient health information and other sensitive data. Respondents worry about data breaches, member identity theft, data leakage, and inappropriate use of data, especially if there is “inadequate governance over AI deployments.” “I worry that employees won’t get enough cybersecurity training,” says one respondent. “Even with AI, human mistakes can still lead to data breaches.”

Insufficient technological protections can raise those fears, as some respondents worry about “weak identity and access management for AI systems” and “insecure API integrations between AI platforms and healthcare systems.”

Some express concern about the integrity of AI learning models, such as “generative models accidentally storing specific patient names or Social Security numbers in their training data,” “data poisoning altering critical diagnostic machine learning models,” or “bad actors reverse-engineering AI outputs to extract the private medical records used to train the model.”

Respondents also note the “difficulty [of] auditing AI-driven systems” as well as “regulatory compliance challenges.”

And they worry that humans and their systems simply won’t be able to keep up, especially if the technology is employed by bad actors. “The biggest fear is that AI accelerates attacks faster than human teams can defend them,” says one respondent.

Sample responses:

Payers / health plans

- “AI accelerating the sophistication of cyber criminals”
- “Insufficient security controls around AI tools”
- “Manipulated clinical decisions or claims adjudication at scale”
- “Regulatory compliance, including PII, state privacy regs and HIPAA compliance”
- “Understanding emerging threats, balancing appropriate levels of prevention and response against business needs and competitive threats”

Providers

- “Data privacy, data loss, malicious injects”
- “Mass inappropriate denials bundling by payers”
- “My biggest concern is patient data privacy. Healthcare organizations handle a lot of sensitive information, and if AI systems aren’t properly secured, the impact of a data breach could be huge.”
- “Reliability, integrity of the AI service, and costs”
- “From a leadership perspective, cybersecurity is not just an IT responsibility. Operations, compliance, IT, clinical teams, and revenue cycle leaders all share accountability. Organizations need strong governance, clear AI usage policies, employee education, continuous monitoring, and regular security assessments to safely realize AI’s benefits. I believe AI can significantly improve healthcare operations, but only if security, privacy, and compliance are built into every stage of implementation—not added afterward.”

CONCLUSION

The data tells us that AI adoption is moving faster than the governance, security and operational infrastructure required to support it. With more than 90% of respondents expecting AI and/or cybersecurity investment to increase, it's not a matter of whether healthcare will adopt AI, but whether organizations can build the governance, security and infrastructure needed to scale it responsibly.

MedCityNews

About MedCity News

MedCity News is the authoritative source for what's next in the business of healthcare. Today's healthcare industry requires smart collaborations across sectors. MedCity News provides timely breaking news and analysis in order to inform decision making and highlight opportunities for better business connections. Our thought leaders range from healthcare CIOs and pharma CEOs, to payers and providers, to venture capitalists and healthcare's next great entrepreneurs.



About Cotiviti

Cotiviti's infrastructure platform enables healthcare organizations to deliver better care at lower cost through advanced technology and data analytics that improve the quality and sustainability of healthcare in the United States. Cotiviti's solutions increase transparency and collaboration between payers and providers while empowering them to reduce medical and administrative costs, enable better health, improve claims payment efficiency, streamline operations, drive interoperability and advance value-based care. Its customers serve the majority of U.S. healthcare consumers, providing coverage and care for over 300 million members and patients. For more information, visit www.cotiviti.com.

Contact Us

To learn more about MedCity News, visit our website at MedCityNews.com. If you would like to be part of future research opportunities, please contact: Ken Montgomery, MedCity News Publisher, at kmontgomery@medcitynews.com.