DRUMMOND

SECURING AI

CREATING ADOPTION-READY HEALTH IT SOLUTIONS

Market Study: AI in Health IT Risk Management

Published June 2025 |

TABLE OF CONTENTS

EXECUTIVE SUMMARY

It's obvious AI is rapidly gaining momentum in health IT. What's less obvious is how ready the industry is for the AI revolution. While enthusiasm is high among healthcare providers and EHR developers, many are still figuring out how to assess, develop, and manage AI tools to ensure responsible, safe, and effective use.

This report reveals a meaningful gap between AI interest and AI readiness. Healthcare organizations aim to enhance documentation, alleviate burdens, and improve decision-making, but they also face challenges such as policy uncertainty, inconsistent oversight, and internal capacity limitations. Many are looking to the AI developers and vendors they work with to help fill those gaps.

For health IT AI developers, this is a pivotal moment. There is a real opportunity to lead not only with features but with clarity, support, and credibility. Whether you are the developer of clinical decision support, ambient listening, or automation tools, or an EHR or healthcare provider choosing to partner with a solution vendor, this report will help you understand the trust signals stakeholders and customers are seeking and the challenges they need help overcoming.

The insights that follow provide a practical perspective on market timing, adoption challenges, and the increasing expectations placed on AI developers and vendors in healthcare.

Key findings include:

Figure 1: Executive Summary Key Findings

METHODOLOGY

Drummond conducted a survey in April 2025 to gather directional insight into how health IT organizations, particularly ONC Health IT Certified EHR developers and healthcare providers, are approaching AI adoption, governance, and risk management. The survey was distributed to professionals with relevant oversight or operational roles related to AI, compliance, privacy, product development, and clinical or technical integration.

Participants responded to a structured set of questions exploring current AI usage, governance readiness, perceived risks, mitigation measures, and anticipated growth in AI deployment. The survey findings are based solely on the participants' responses and are not statistically representative of the entire industry. However, the results provide valuable insights into the mindsets, gaps, and expectations shaping AI risk management and adoption today.

Participant Overview

Survey participants represented a cross-section of leadership and functional roles within their organizations. These included:

- Product and technical leaders involved in the development and integration of AI tools within health IT systems
- Compliance and security officers (especially from EHR developers) responsible for ONC Health IT Certification requirements and organizational risk governance
- Clinical and operational leaders from healthcare providers who assess AI tools based on patient safety, workflow impact, and regulatory obligations
- Executive decision-makers who influence or directly oversee technology adoption, integration strategy, and procurement

The diverse backgrounds of participants reflect the multi-disciplinary nature of AI implementation in healthcare, where strategy, compliance, clinical impact, and technical feasibility all play critical roles.

AI ADOPTION FORECAST

Eighty-eight percent (88%) of EHR developers and healthcare provider participants expect their organization's own use of AI to increase over the next two years (Figure 2). This AI growth signal was split evenly between those expecting a moderate increase and those expecting a significant increase. Only 6% of participants reported no plans to expand AI usage.

This outlook shows strong confidence in AI's value to EHR developers, healthcare providers, and their customers. While the expected pace and scale of adoption may vary, the directional consensus reflects growing interest in using AI to support clinical documentation, administrative processes, and product enhancement.

Anticipated AI Use Over the Next Two Years

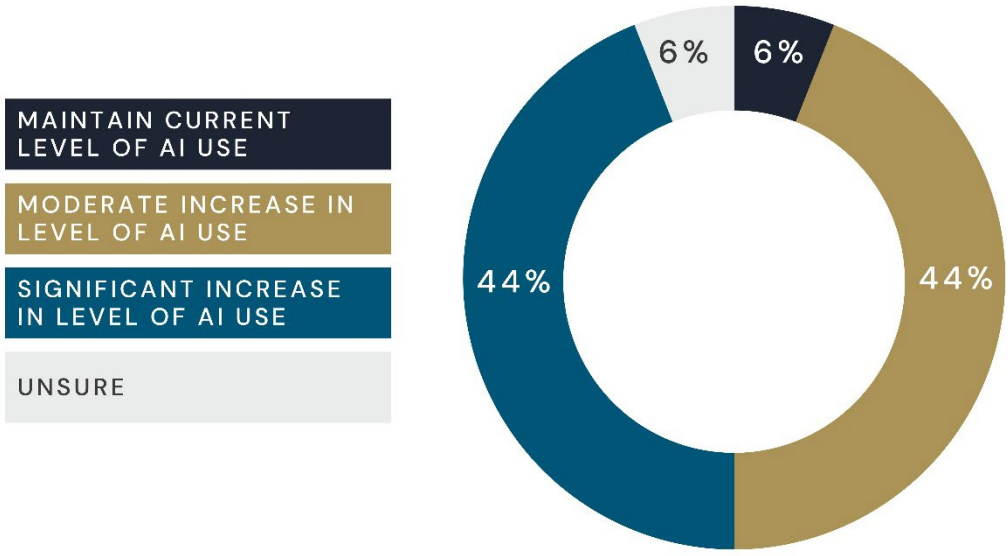

Figure 2: Do you anticipate your own organization's use of AI will increase over the next two years?

The optimism is notable given the early stage of many organizations' AI programs. This planned growth also raises questions about readiness, particularly when viewed alongside findings about the lack of risk governance programs (see Figure 8), limited policy awareness, and a high dependence on vendors for compliance. *These disconnects may present both a market opportunity and an implementation challenge for AI developers aiming to support secure and sustainable AI adoption.*

Strategy and Adoption – Healthcare Providers

AI adoption among healthcare providers remains relatively limited, with most respondents indicating low current usage levels (Figure 3). Among those utilizing AI, the top use cases include workflow automation, medical imaging analysis, and ambient listening for clinical documentation purposes. These applications suggest that when AI is adopted, it is often aimed at supporting efficiency, improving diagnostic workflows, or reducing the burden on clinicians. The response may have been influenced by the existing broad availability and early adoption of transcription and summarization capabilities.

Use of AI in Operations Related to Patient Care

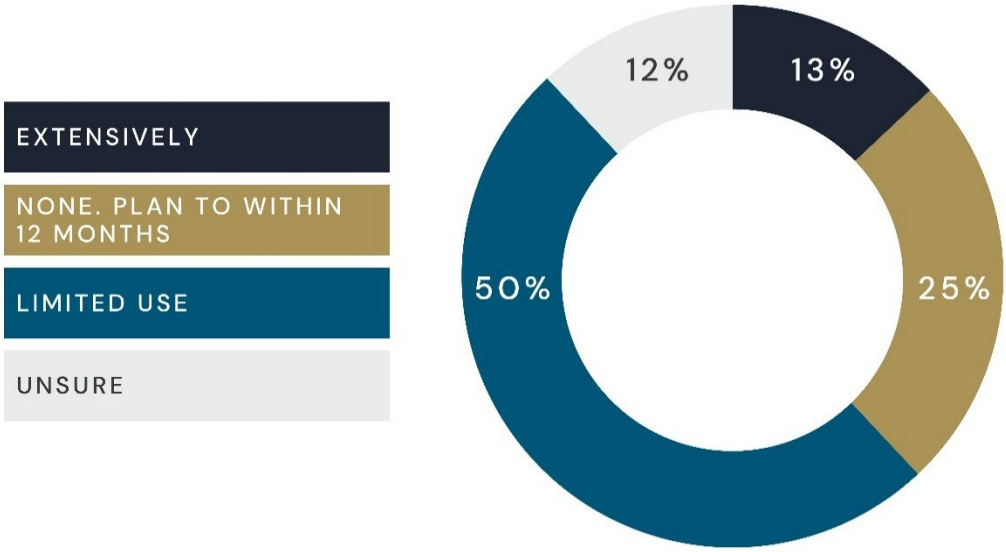

Figure 3: Is your organization currently using AI in its operations related to patient care?

Regulatory constraints emerged as key barriers to broader adoption. Participants identified HIPAA and state-specific privacy laws as significant hurdles that restrict the use of AI tools in terms of how and when they can be utilized. In this context, it is noteworthy that approximately 75% of provider respondents said they rely on their vendors to ensure security and compliance requirements (Figure 4). This high level of reliance creates an opportunity for AI developers to offer turnkey solutions that address compliance concerns up front.

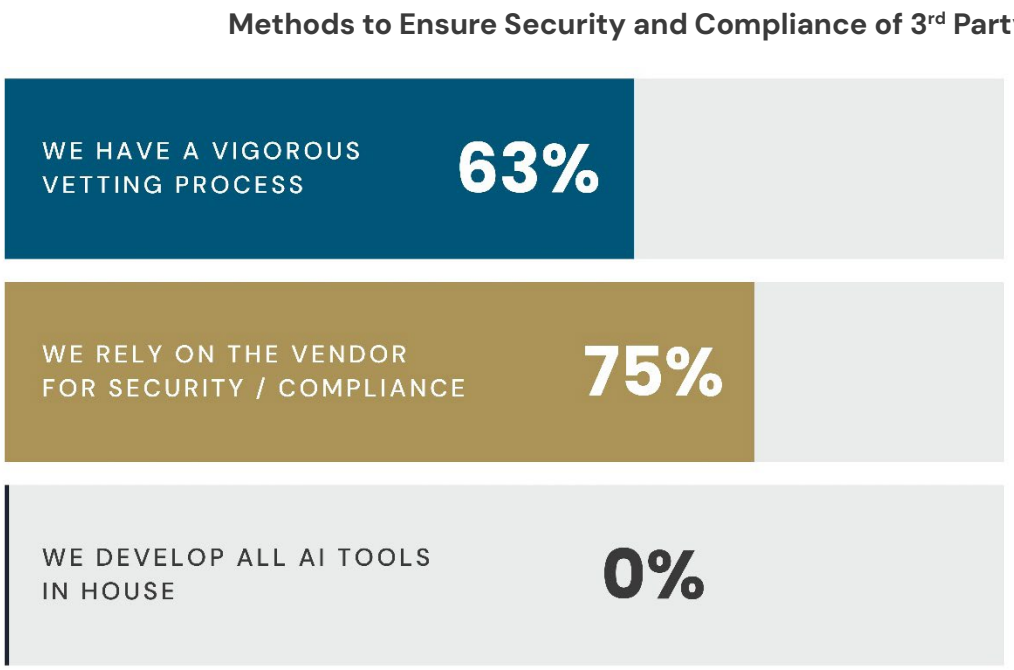

Figure 4: How do you ensure the security and compliance of the 3rd party AI plugins you are currently using? Select all that apply.

Strategy and Adoption – EHR Developers

EHR developers expressed a strong interest in expanding AI capabilities in the near term. Eighty-five percent (85%) of participating EHR developers said they plan to release AI functionality within the next two years (Figure 5). Only a small portion reported having AI solutions currently in development; however, most remain in the ideation or planning phase. This gap highlights the low maturity stage of AI development among many EHR developers as well as their need to rely on AI vendors for solution development.

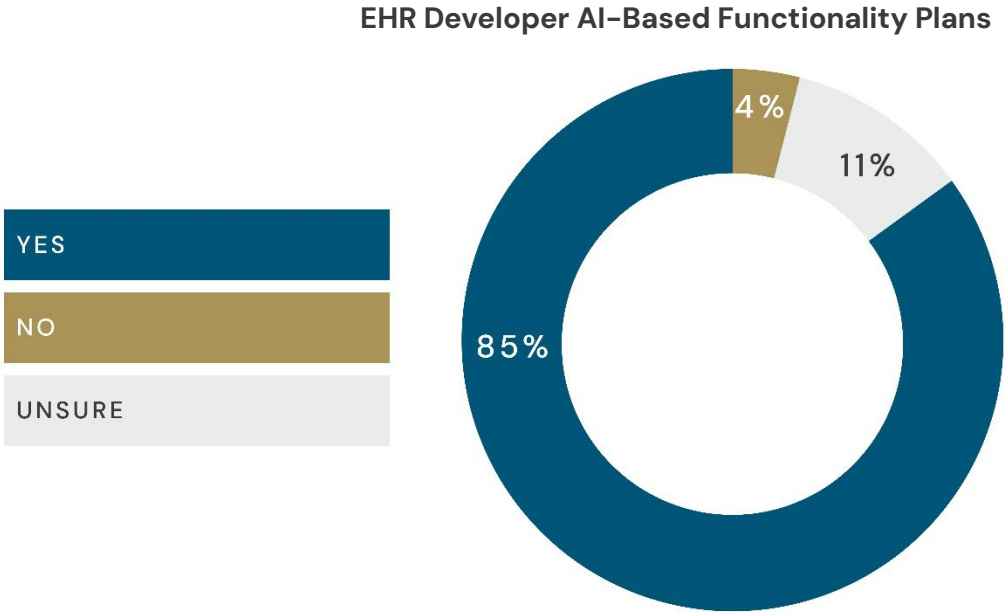

Figure 5: EHR developers planning to release AI-based functionality within the next two years.

The majority of EHR developer participants (57%) plan to partner with third-party AI providers rather than build functionality entirely in-house (Figure 6). Additionally, 75% indicated they use or will use the HL7® FHIR® standard [often in combination with Consolidated Clinical Document Architecture (C-CDA) and other protocols] to integrate with AI solutions (Figure 7), which may reflect alignment with ONC Health IT Certification Program requirements more than deep integration. The varied maturity of FHIR implementations could impact the ease of integrating AI tools into existing systems, making interoperability and technical readiness key differentiators for AI vendors targeting this audience.

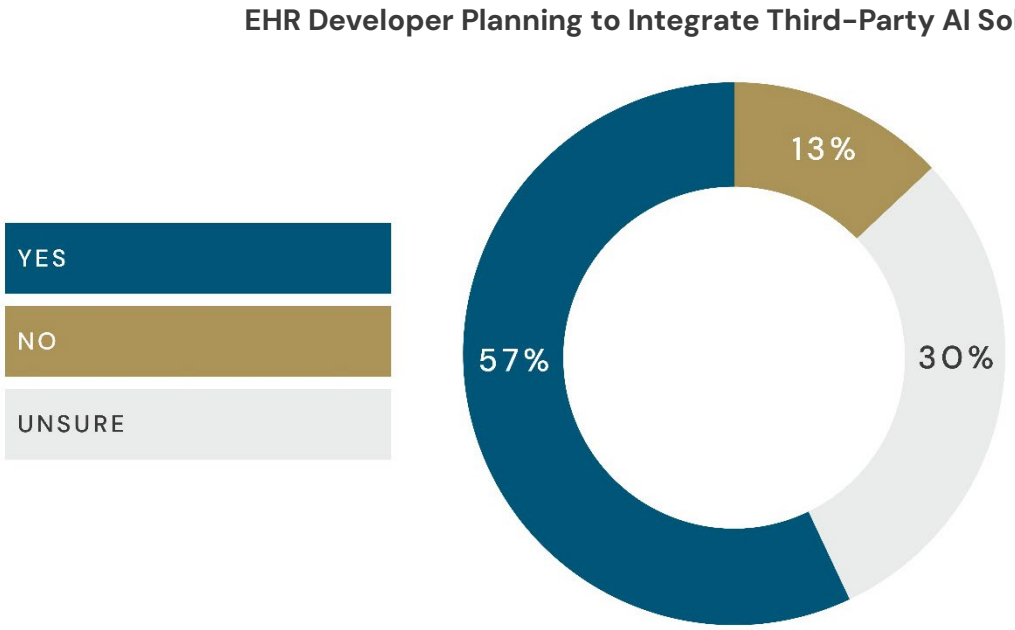

Figure 6: EHR developers who plan to use 3rd party solutions to provide their customers with AI-based functionality.

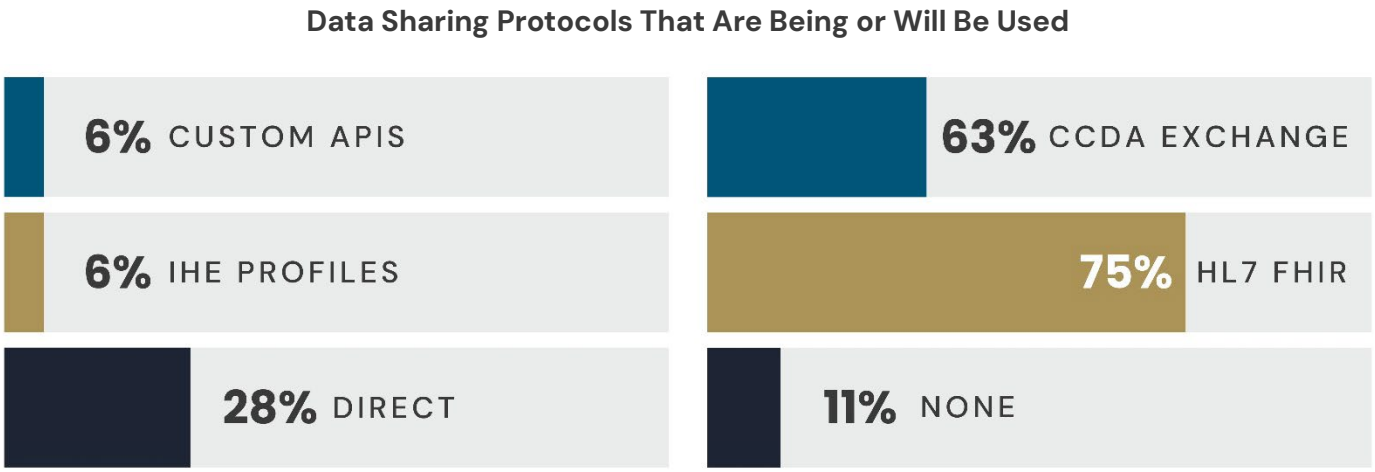

Figure 7: Data sharing protocols participants use or plan to use. Participants were asked to select all that apply.

These insights highlight a significant window of opportunity for AI developers to support EHR developers with modular tools, integration support, and compliance resources tailored to meet the ONC Health IT Certification Program requirements and market expectations.

www.drummondgroup.com
(877) 437-8666

AI RISK GOVERNANCE IN HEALTH IT

AI risk governance programs exist—but awareness is weak. While some organizations report having AI risk governance or risk management programs in place, 36% of participants (EHR developers and healthcare providers) were unsure whether their organizations have such programs. This disconnect between formal policies and internal awareness presents an opportunity for AI developers to help clarify and reinforce best practices for risk governance and management. Without a clear understanding of each stakeholder's role in maintaining compliance with AI risk governance policies and procedures, organizations may unintentionally increase risk or face compliance gaps.

AI Risk Readiness

Over two-thirds of participants (70%) reported that their organization either lacks a formal AI risk governance program or that they were unsure if one existed (Figure 8). This gap suggests that AI risk governance is not yet fully embedded within organizational governance structures, particularly in healthcare environments. The importance of AI risk governance may not yet be widely acknowledged or supported by strong compliance drivers—unlike more mature requirements in security and privacy domains (e.g., HIPAA, PCI).

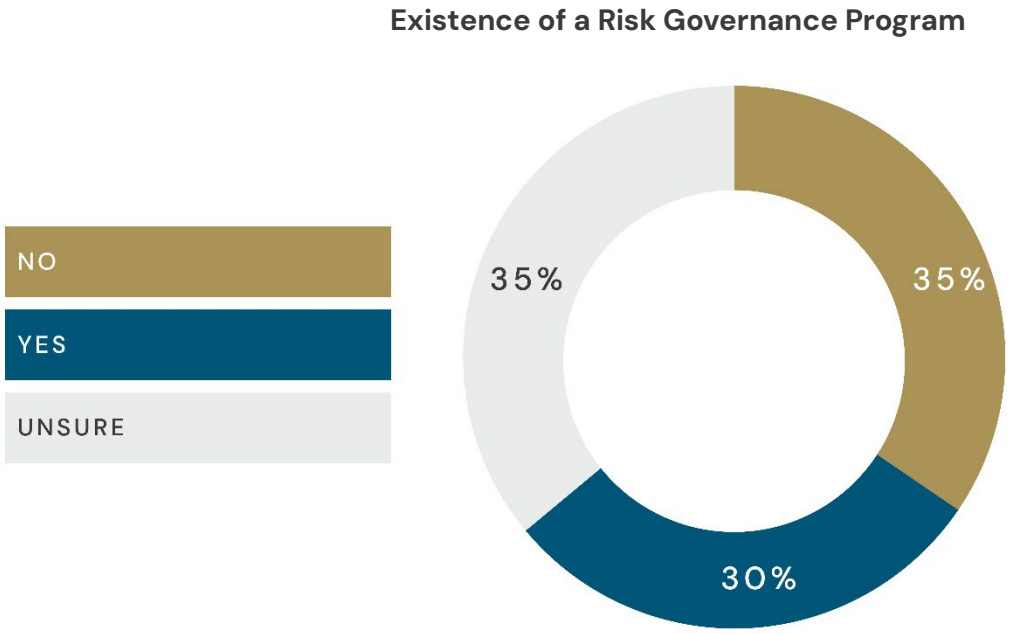

Figure 8: Does your organization have a risk governance program?

Among those with programs in place, only 42% reported updating policies frequently (monthly or quarterly). EHR developers were more likely than healthcare providers to have established governance programs and to update policies regularly (Figure 9). This possibly reflects their regulatory obligations tied to the ONC Health IT Certification Program [e.g. 170.315 (b)(11)] and other state-level regulatory requirements. For AI developers, this suggests an opportunity to position their products or services as governance-supportive, especially when engaging with healthcare provider organizations.

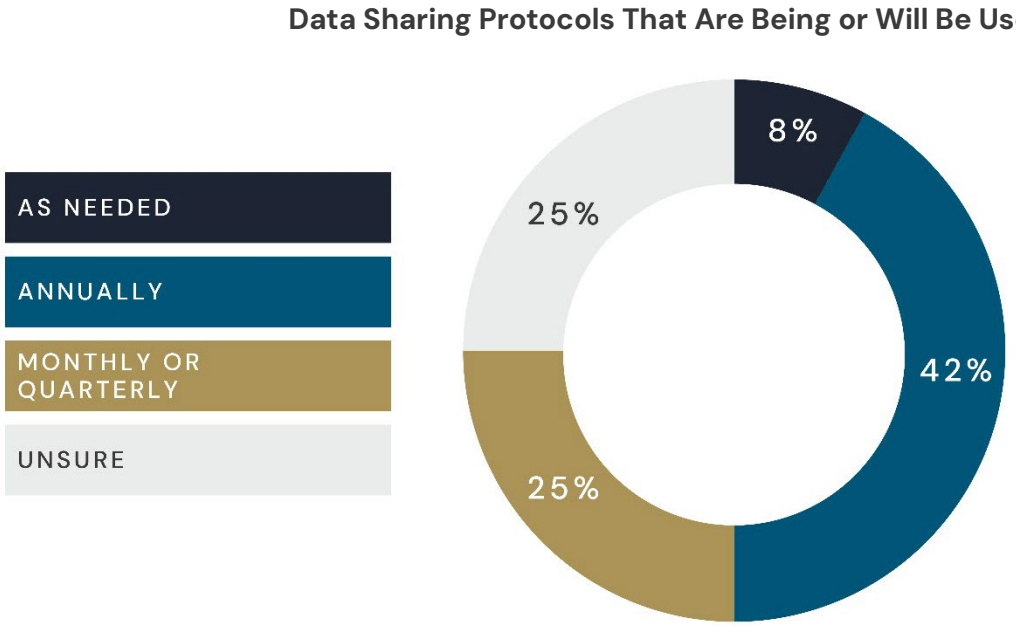

Figure 9: How frequently does your organization update AI risk governance policies?

Risk Mitigation Measures

When asked about actions taken to manage AI-related risk, healthcare providers most often pointed to data privacy controls, cybersecurity programs, and the presence of organizational governance systems (Figure 10). EHR developers reported those same three priorities, but also emphasized the use of Large Language Model (LLM) filters and formal risk frameworks.

This distinction indicates that EHR developers may operate with greater technical sophistication, while healthcare providers may focus more on regulatory and operational safeguards (specifically driven by HIPAA security requirements). AI developers serving both segments should be prepared to support different priorities, provide clear explanations of how their tools address each, and provide proof of their own risk governance practices.

Measures Healthcare Providers & EHR Developers Are Taking to Manage Potential AI-Related Risks

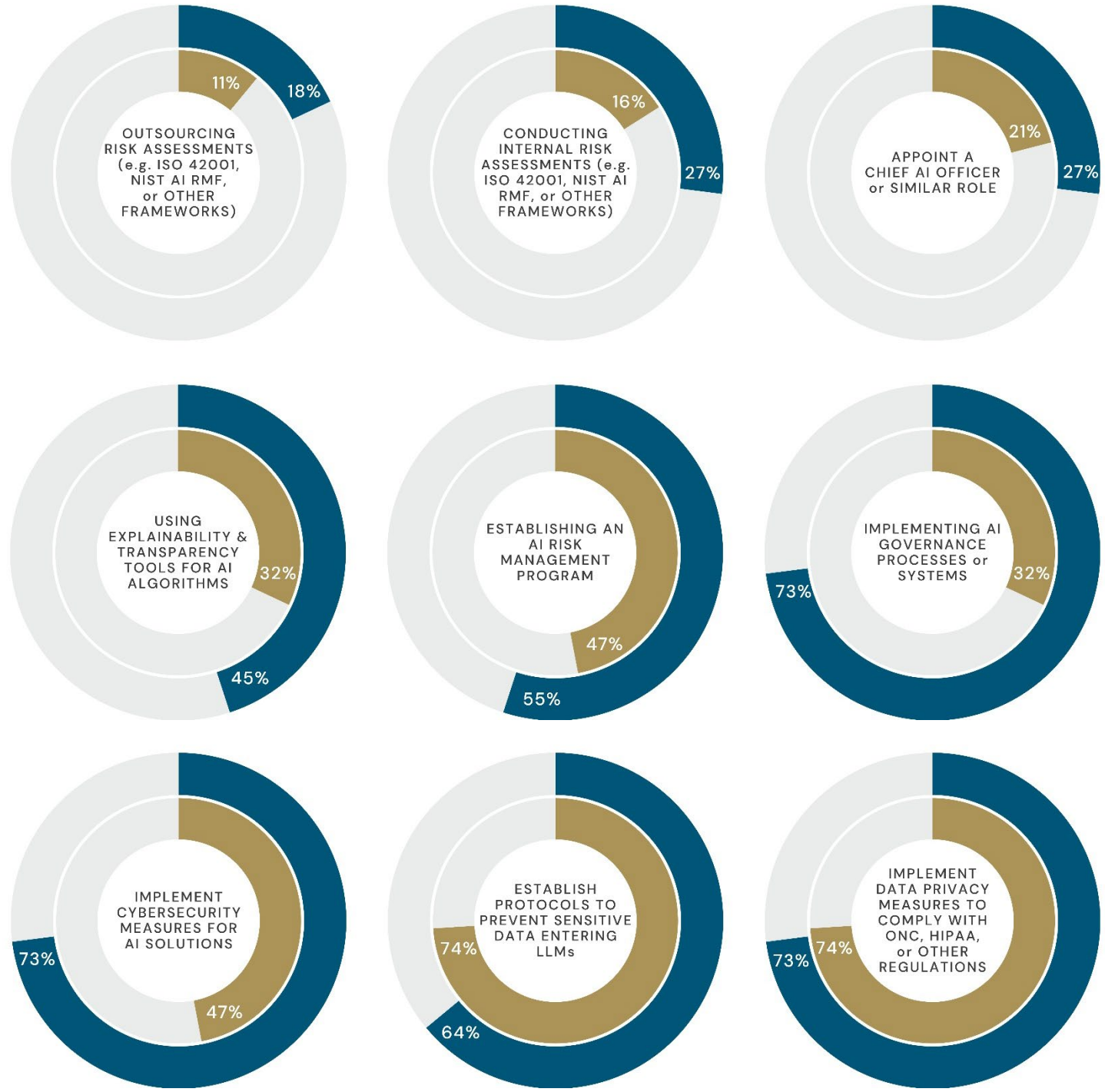

Figure 10: What measures is your organization taking to manage potential AI-related risks?

Use of Publicly Available AI Tools

Participant responses revealed inconsistent approaches to employee use of public AI tools (e.g., ChatGPT, Copilot, Bard). While 62% of participants said their organizations restrict employees, allowing them to use only approved tools, 38% were either unaware of the policy documentation or indicated that such policies did not exist (Figure 11). The use of publicly available AI tools without prior assessment increases the risk of confidential information being disclosed to and utilized by LLMs.

Employee Use of Publicly Available AI Tools

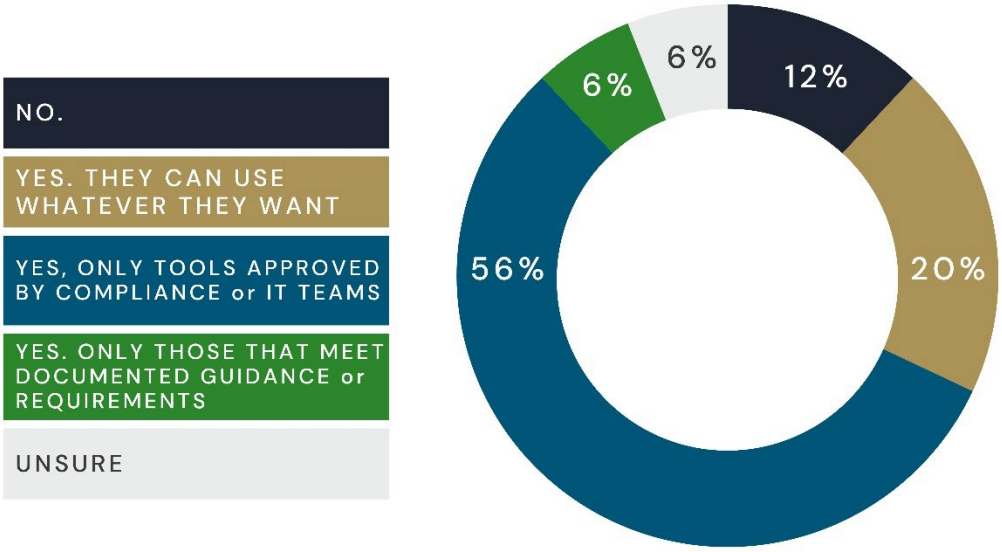

Figure 11: Does your organization allow employees to use publicly available AI tools?

Top Challenges in Managing AI Risk

Participants identified and were asked to rank by severity several recurring challenges when it comes to managing AI risk (Figure 12 and Figure 13). These challenges include:

- Data privacy and security compliance requirements
- Addressing bias and fairness in algorithms
- Shortage of skilled internal resources
- Vulnerability to security threats
- Limited trust in AI-generated results (especially among developers)

Each of these challenges presents a point of differentiation for AI developers. Solutions that are transparent, configurable, and well-documented may offer a competitive edge, particularly if they help customers overcome technical limitations or regulatory concerns.

Healthcare providers shared that almost all the consideration options provided were moderate to critical challenges, indicating providers want robust, comprehensive solutions that address their concerns. Healthcare providers are acutely aware of their immediate need to implement industry-led technical solutions to continue providing safe and optimal patient care (Figure 12).

Challenges Addressing AI Risk - Healthcare provider responses:

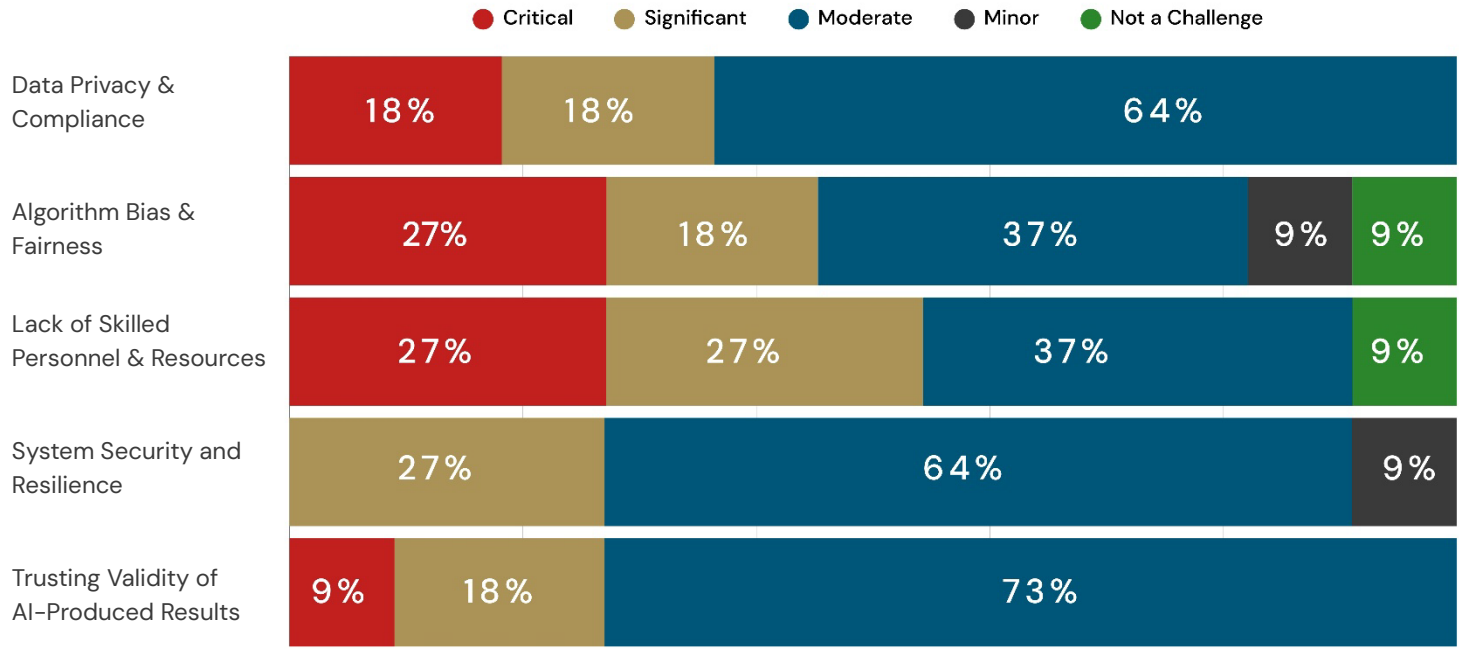

Figure 12: Rank the challenges your organization faces in managing AI risk. Healthcare provider participant responses.

A noteworthy takeaway is that EHR developers are very concerned about the quality of data produced by these tools. In contrast, providers are more likely to trust the generated data once it is implemented (Figure 13). This shows that providers themselves are more likely to trust the quality of the technology after choosing the right solution for their needs.

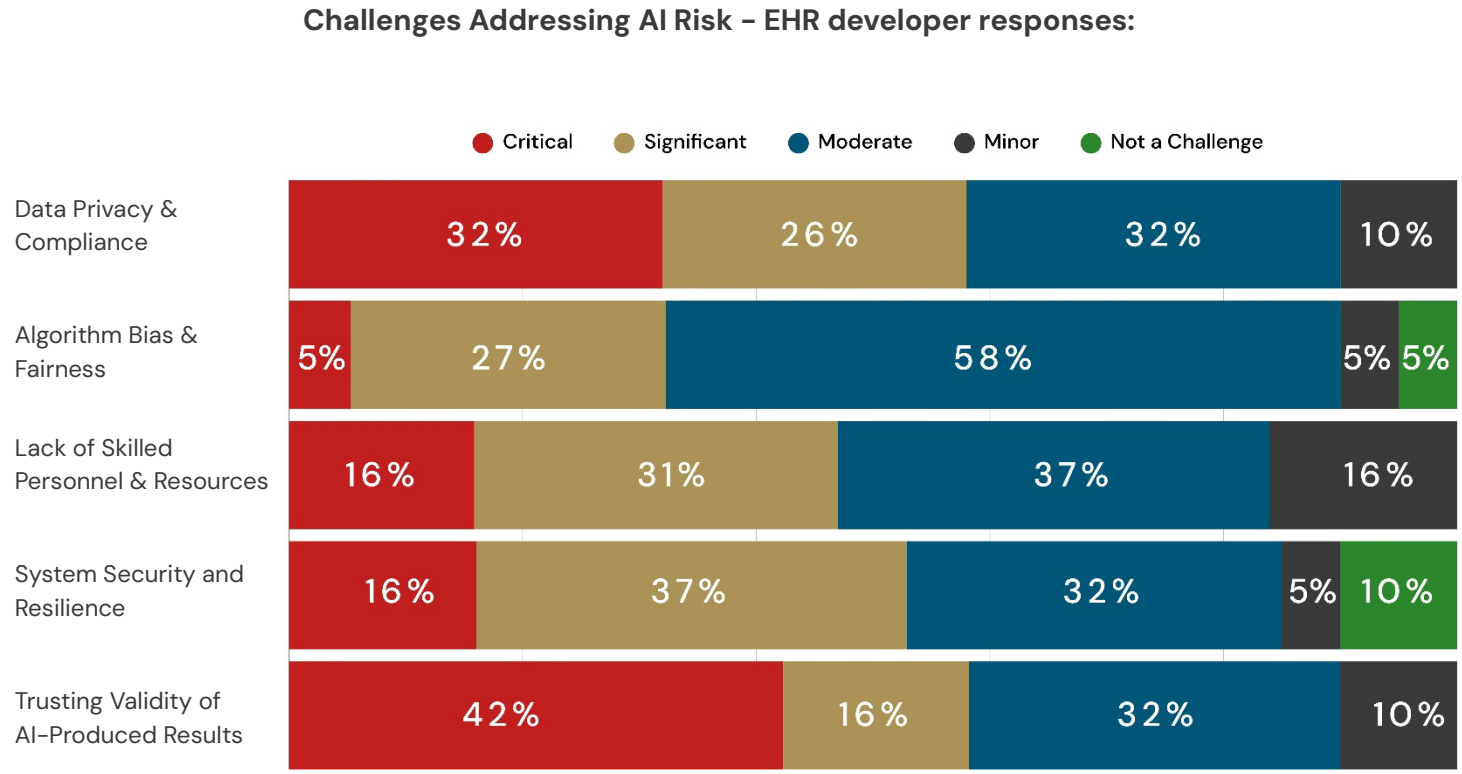

Figure 13: Rank the challenges your organization faces in managing AI risk. ***EHR developer participant responses****.*

STRATEGIC RECOMMENDATIONS FOR HEALTH IT AI DEVELOPERS

Health IT AI developers are uniquely positioned to support safe, scalable adoption by anticipating the needs of both EHR developers and healthcare providers. Based on participant feedback, the following opportunities stand out:

- **Build Trust Through Governance, Oversight, and Design**: Health IT AI developers have a unique opportunity to shape how organizations manage AI safely and credibly. Trust is built not just through outcomes, but through the structure, transparency, and integrity of the product itself.
    - Support governance readiness by including built-in compliance and policy features such as documentation, permissions, and audit settings.
    - Enable operational oversight with controls that help organizations manage usage transparency, internal audits, and patient data protection.
    - Embed safeguards in design that address bias, explainability, and security—strengthening your product's trust profile from the inside out.
- **Address AI Application Security:** Health IT developers should recognize that traditional and novel security concerns extend into the AI solution space, and will continue to be a key trust issue supported by mature compliance requirements.
- **Help EHR Developers Deliver AI Faster:** Many EHR developers plan to introduce AI functionality, but are still early in the process. Easy-to-integrate modules or white-label functionality can help them reduce time to market while remaining aligned with certification standards.
- **Tailor Features and Messaging by Audience:** For EHR developers, focus on ease of integration, transparency, and regulatory alignment. For healthcare providers, emphasize built-in controls, risk documentation, and compliance support.
- **Design for Limited Internal Capacity:** Both audiences struggle with resource gaps. Developers who offer managed services, turnkey configurations, training support, or minimal setup requirements will stand out.
- **Ensure Baseline Interoperability:** The EHR developer community, driven by increased demand, regulation, and certification, is well-positioned to support HL7 FHIR. While implementations vary, an AI solution that leverages FHIR will be viewed as more competitive and compatible by the marketplace.
- **Strengthen Credibility Through Third-Party Validation:** Consider voluntary risk assessments, compliance audits, and testing or certification programs that demonstrate alignment with industry standards. These third-party validations can support procurement decisions, reduce perceived risk, and improve market access.

DRUMMOND

FREE Drummond Consultation

Learn how health IT AI modules and FHIR Client Apps can demonstrate compliance and trustworthiness.

www.drummondgroup.com | sales@drummondgroup.com | 877-437-8666

Published June 2025 |