Shadow AI:
A hidden risk to healthcare

As AI tools proliferate the healthcare industry, a new Wolters Kluwer Health survey highlights how clinical and administrative teams are using unauthorized solutions and introducing organizational risk. Health leaders urgently need insights into which tools are being used and to establish clear enterprise-wide solutions and policies—for safety and privacy.

Wolters Kluwer

Shadow AI is an immediate risk for healthcare leaders

Technology leaders are no strangers to shadow IT challenges, which occur when internal teams adopt applications or hardware without support or organizational approval. In many cases, these violations stem from employees trying to improve their workflows and operate more efficiently. However, inconsistent tools can create security oversight challenges and expose organizations to security breaches and data privacy violations, impacting customer trust and incurring costs.

The latest threat is "Shadow AI," where teams adopt different AI-powered tools and chatbots without proper approval processes, posing risks and challenges for healthcare leaders well beyond the IT department. As AI rapidly develops, new solutions are harnessing this innovation and coming to market, providing a variety of options to address workflow tasks and support information gathering. Healthcare providers are at the forefront of this challenge—one survey revealed that **58%** of frontline health system staff used generic, free AI tools for work at least once in the previous month, with **39%** using AI weekly or more.[1]

With these challenges in mind, Wolters Kluwer Health sponsored an online survey among 518 full-time healthcare professionals—both providers and administrators—on their perceived usage of AI tools and to identify gaps in risk tolerance and shadow usage.[2] In the survey, **40%** of respondents had encountered an unauthorized AI tool in their organization but did not use it. An additional **17%** admitted to using an unauthorized AI tool.

The results reinforced industry findings: **Clinical and administrative teams want to adhere to rules surrounding AI usage, but if the organization hasn't provided guidance or approved solutions, they'll experiment with generic tools to improve their workflows.** This can expose the organization to security, data, and patient safety risks.

The good news is that healthcare organizations can help mitigate these risks by establishing enterprise-wide guidelines for AI tool usage and communicating these policies to their teams, fostering a safer, more efficient, and more secure technology future.

"In 2025, shadow AI surged across healthcare organizations, as staff across all aspects of care sought ways to improve efficiency amid persistent burnout, staffing shortages, and other factors. As a result, in 2026, healthcare leaders will be forced to rethink AI governance models and implement more formalized organization-wide frameworks that ensure the responsible use of AI, including proper training around the technology and appropriate guardrails to maintain compliance."

Alex Tyrrell,
Senior Vice President and Chief Technology Officer, Wolters Kluwer

Operating in the dark: Shadow AI risks transparency and safety

Health systems are feeling operational and financial crunches, including funding cuts, increased administrative work, and clinician shortages. One study estimated that primary care physicians need an impossible **26.7 hours** per day to provide guideline-recommended care.[3] Healthcare professionals simply need more time and fewer administrative tasks to meet patient care requirements.

Healthcare has traditionally lagged behind other industries in adopting technology, even if it creates wider efficiencies or supports data sharing. However, it has rapidly adopted AI tools—at more than twice the rate compared to other industries—highlighting the need for urgent responses to rising costs, labor shortages, and shifting patient expectations.[4] These tools offer a wide range of services, from office administration support to patient portal chatbots to generative information searching. A modern, fast, digital patient and clinician experience is now a competitive differentiator, and AI adoption has become a mix of opportunity and survival.

However, in many cases, adoption and innovation are outpacing policy and enterprise decision-making, leading employees to use any tool they can get their hands on to accomplish their tasks. When this happens, system leadership loses the ability to regulate or have full security oversight of tools within the organization, and clinical leaders have greater concerns about variations in care resulting from disparate tools.

$7.42M USD

Average cost of AI security breaches for the healthcare industry in 2025

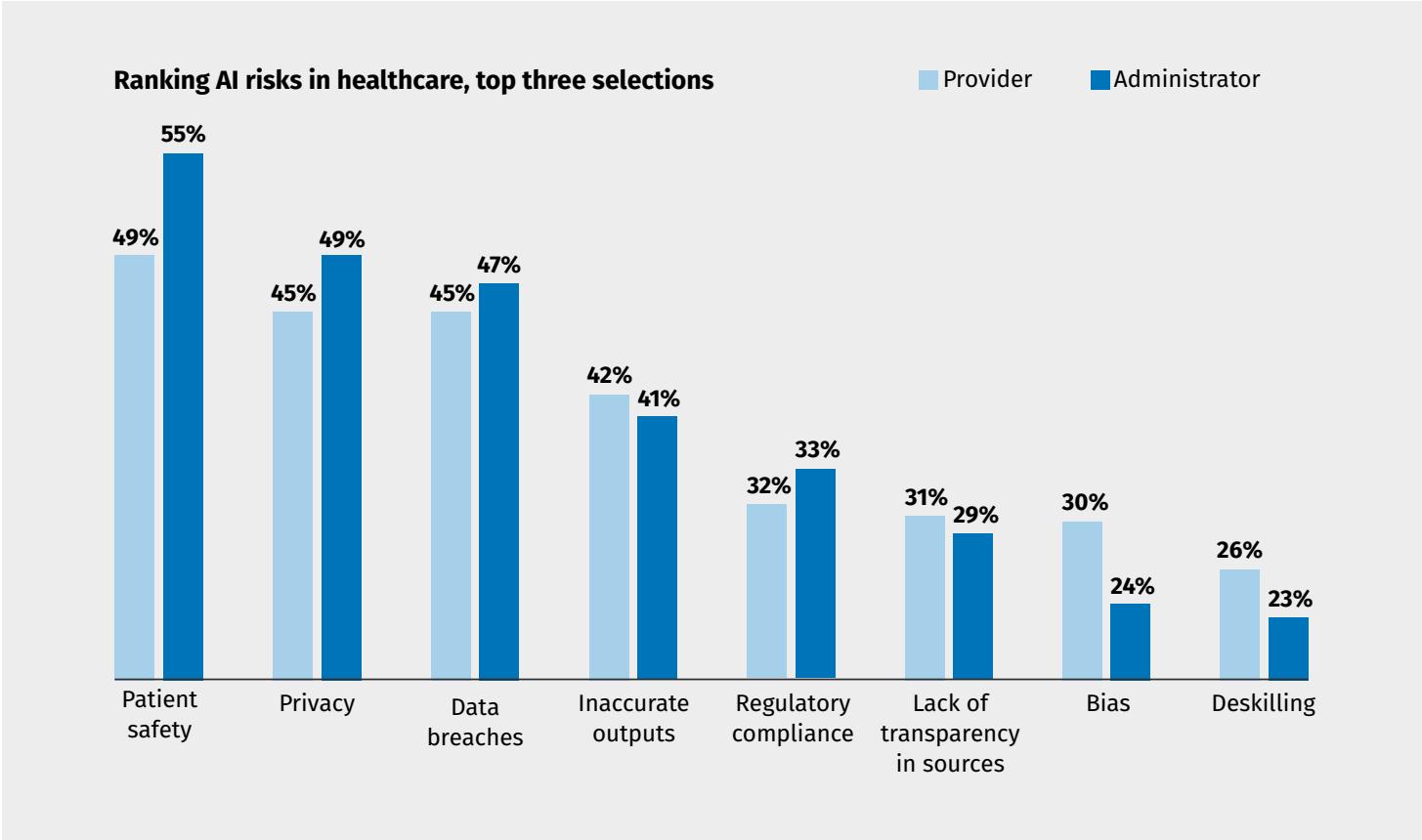
57%

of respondents had encountered or used an unauthorized AI tool in their organization

A booming technology space can introduce risks to data and patient safety

Using unsanctioned AI tools can have wide-ranging—and costly—impacts. A 2025 IBM study identified that **97%** of organizations that had had an AI-related security incident to their models or applications had lacked proper AI access controls, and **63%** of organizations surveyed lacked AI governance policies.[5] The average security breach in the healthcare industry totaled over **$7.4 million** in 2025, and takes the longest to identify and contain.

The Wolters Kluwer Health survey reflected these concerns. When asked to rank a series of AI risks to healthcare, both providers and administrators selected patient safety, privacy, and data breaches as the top concerns.



Within the healthcare space, generic AI tools—especially generative AI and chatbots—can pose more serious risks for organizations if they are embedded within patient data applications or used for clinical decision support. These tools can still run the risk of hallucinations, inconsistencies, and biases, bringing risks to patient safety, HIPAA violations, and compliance concerns.[6] Even in cases where patient data has been de-identified to protect privacy, some tools re-identify datasets, potentially allowing data to be relinked to the individual.[7]

If generic AI solutions aren't grounded in evidence and pull information from broad sources, they can lack transparency and introduce bias and risk into the clinical decision-making process. Understanding the black box of AI—how it generates outputs or recommendations—is critical for any healthcare organization, especially if the tool interacts with patient care decision-making. Leaders who don't properly analyze this run the risk of selecting a tool that can impact the enterprise or that can create variations in care.

Ultimately, addressing shadow AI is not about restricting access to productivity tools. Leaders must understand why teams are using unsanctioned tools and which challenges they're trying to solve, and then identify enterprise-level tools that can accomplish these goals safely and securely.

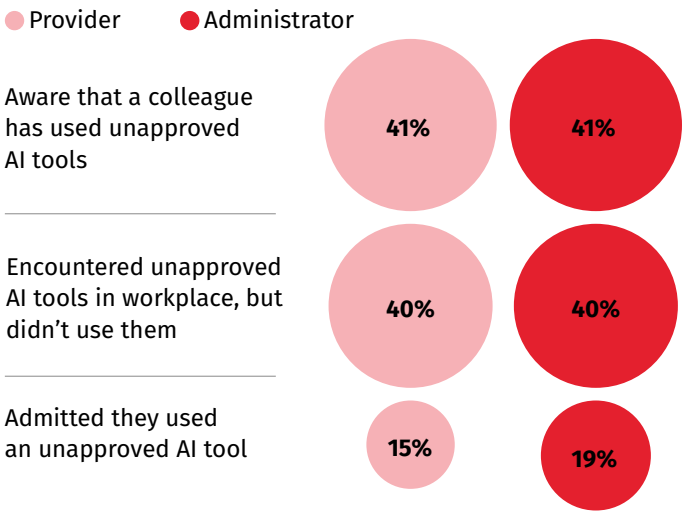
> *"My biggest concern is ensuring that AI tools are safe, accurate, and compliant. Particularly that they do not compromise patient safety, privacy, or regulatory compliance."*
>
> **IT Executive, Health System, 5-19 years of experience**

Survey findings: Three key gaps in AI tool usage

The Wolters Kluwer Health survey on shadow AI highlighted some key gaps between health system administrators and providers in tool usage, risk tolerance, and perceptions of policy communications.

When it came to using unsanctioned AI tools, the survey showed **40%** of all respondents had encountered them in the workplace but didn't use them, and nearly **17%** reported using unapproved tools themselves. When respondents were asked why they used unapproved AI tools, almost **50%** did so for a faster workflow, and 1 in 3 pointed to either a lack of approved tools or the approved tools lacking the desired functionality.

Key gaps in AI tool usage



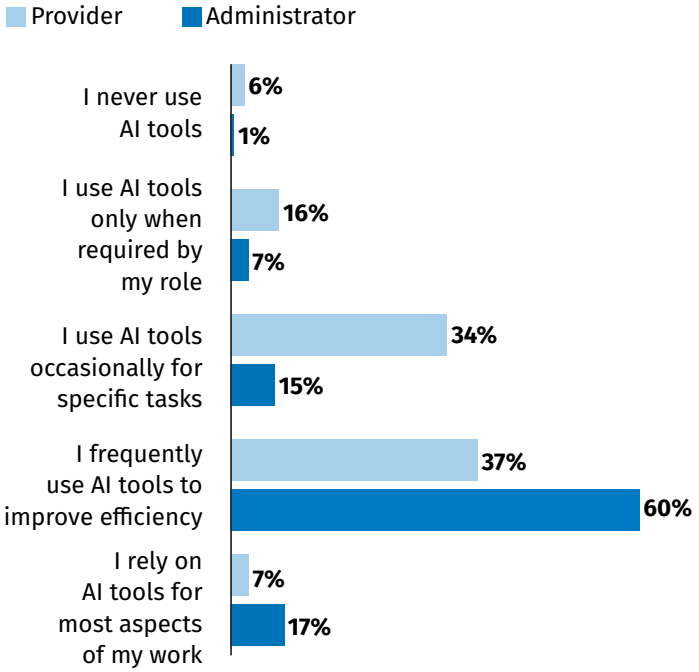
#1: Administrators are more optimistic about AI's impact

When asked if they believe AI will significantly improve healthcare within the next five years, administrators expressed more optimism than providers. The largest split was **48%** of administrators and **34%** of providers selecting "strongly agree" as a response, and **16%** of providers were "neutral" compared to just **6%** of administrators.

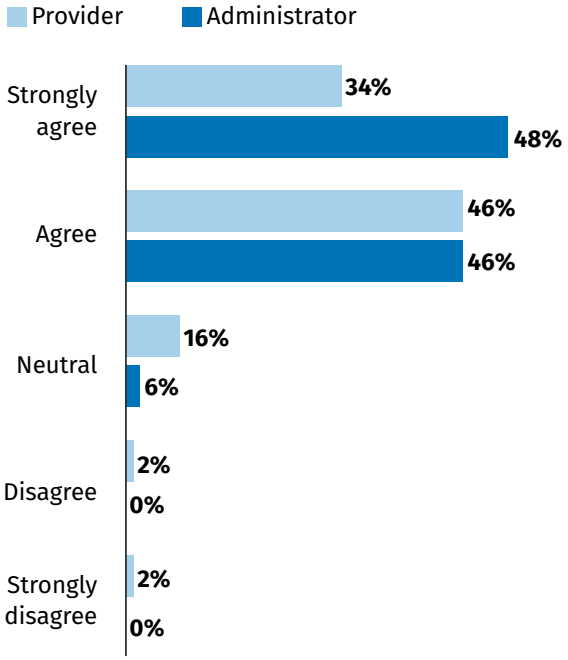
Administrators also used tools more frequently for efficiency in their daily work. They ranked higher in using AI for data analysis, predictive analytics, and administrative tasks. Providers were most likely to use AI for data analysis, patient scheduling, and patient engagement.

> *"My greatest expectation for medical AI is to enable access to high-quality medical resources (such as AI image diagnosis) in remote areas, thereby narrowing the gap in medical care between urban and rural areas."*
>
> **Chief Executive Officer, Hospital, 5-19 years of experience**

How often do you use AI tools in your daily work?



AI will significantly improve healthcare in the next 5 years



#2: Clinicians are more likely to experiment with unsanctioned tools

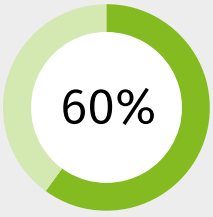
While burnout and administrative burden have been lessening, they still remain at untenable levels.[8] Clinicians are looking for the most efficient ways to support patients and get clinical answers—which often includes using free AI tools that could jeopardize outcomes, security, and possibly introduce patient risk.

One interesting finding was that **26%** of providers who reported using unsanctioned AI tools did so out of curiosity and experimentation, whereas only **10%** of administrators reported the same. This could indicate a higher risk tolerance among providers in getting quicker answers or casually testing out tools that could improve their workflow.

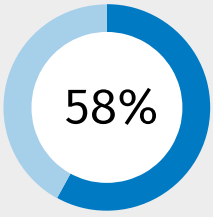
However, providers also ranked patient safety and inaccurate outputs as the top two AI risks, showing there may hesitancy over the tools' ability to meaningfully support their daily clinical work. Interestingly, providers placed a lack of source transparency as the last concern, and for providers with less than five years of experience, bias was ranked the lowest overall. Ranking these topics low in concern is at odds with evidence-based medicine, and highlights the need for thorough AI solution literacy training.

> *"My biggest concern about AI in healthcare is algorithmic bias: If AI systems are trained on datasets that underrepresent certain groups (e.g., elderly patients, racial minorities), they may produce less accurate recommendations for these populations."*
>
> **Resident, Hospital,**
> **Less than 5 years of experience**

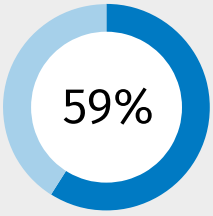
How respondents evaluate AI's trustworthiness



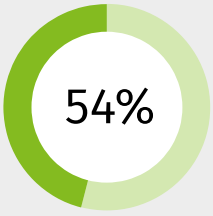
Regulatory approval



Internal testing



Personal review of tool and outputs



External industry reviews and publications

26% of providers who reported using unsanctioned AI tools did so out of curiosity and experimentation

10% of administrators reported the same.

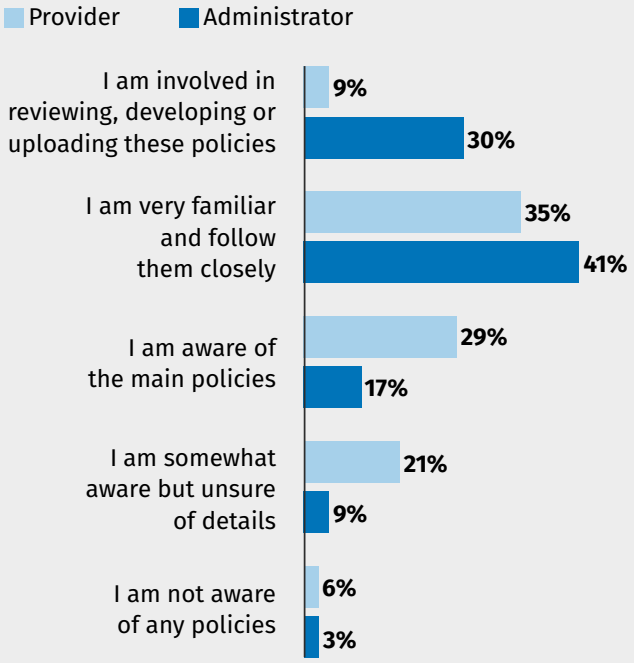
#3: Administrators believe AI policies are strongly communicated—providers, less so

A final gap identified in the survey is how AI policies are created and communicated. Nearly a third **(30%)** of administrators—including those with clinical backgrounds—indicated they were involved in reviewing, developing, or updating AI policies, while only **9%** of providers were.

Administrators were more likely to say they strongly agreed **(42%)** wthat policies were clearly communicated compared to providers **(30%)**. However, **21%** of providers said they disagreed or were neutral on the clarity of communication polices compared to **11%** of administrators.

These differences show that AI policies need to be clearly communicated in multiple locations, not only by email or enterprise communications, but also in point-of-care locations such as the EHR. Training sessions are even more critical as AI is an emerging and constantly evolving technology, and even the most technology-savvy employees may not understand the latest risks and opportunities. Training sessions can also support active learning and policy reinforcement among providers as enterprise tools are established.

How familiar are you with your organization's AI policies?



> *"My biggest hope: That AI quietly bakes reliability into everyday workflows—flagging a sepsis risk an hour earlier, auto-scheduling follow-ups so nothing falls through cracks."*
>
> **Quality Administrator, Hospital, 5-19 years of experience**

Shared AI priorities: Patient safety, security, and accuracy

Understanding where the respondents agreed can help inform policies and strategies addressing shadow AI. When assessing AI risks, both providers and administrators ranked patient safety as the top concern, along with privacy as #3 and #2, respectively. When asked about the top preferred features in AI tools, providers ranked accuracy, security, and reliability as the top three, and administrators selected security, accuracy, and ease of use.

Appealing to these shared values can help when messaging AI policies and enforcing enterprise-wide tools. Ultimately, many within the industry are seeing incredible possibilities with AI. Already, it can improve diagnoses beyond human abilities, such as image scanning, spotting bone fractures, and early disease detection, and support administrative tasks like assessing ambulance needs.[9] With the explosion in technology and innovation, leaders have plenty of tools to consider and test before making enterprise-wide selections.

> *"My biggest hope for AI in healthcare is that it can dramatically improve patient outcomes by making care more personalized, precise, and accessible. For instance, AI could help doctors detect diseases earlier and predict complications before they happen."*
>
> **VP of Quality Administrator, Health System, 5-19 years of experience**

Enterprise AI tools and policies are table stakes for security and consistent outcomes

An enterprise approach to AI solutions will be crucial as healthcare industry leaders look to address their shadow AI challenges. A McKinsey article notes the future of AI in healthcare isn't individual point solutions, it's a modular, connected, and integrated AI architecture.[10]

To successfully and sustainably move forward, organizations have to adopt enterprise-wide AI solutions that are interoperable with existing infrastructure and can mitigate data and security breaches more commonly posed by third-party applications. This can also lessen the shadow burden on IT teams and improve overall governance, and, in the clinical space, can help reduce care variation with consistent information.

For leaders, proactively addressing shadow AI can look like the following steps:

1. **Develop clear AI usage policies**
   Addressing unsanctioned tool usage starts at the policy level. Establish clear risk policies for AI usage and tool approvals that reflect the organization's ethos and business goals, which can be understood across roles and teams. Additionally, include clear processes for regular policy updates as AI technology advances and privacy requirements change.

2. **Foster collaboration between policy decision-makers and users**
   Building a multidisciplinary team of providers and administrators can break down silos within organizations and create a culture of learning and greater collaboration. This can foster greater understanding between administration and providers about key point-of-care challenges, and help gain early buy-in for solution testing and advocating.

3. **Identify purpose-built AI tools that support enterprise-wide security and goals**
   Not all AI tools are created equally or with the same industry-specific attention. Identify how small workflow efficiencies can be achieved with tools, and consider whether a more general administrative tool can suffice or whether a purpose-built solution tailored to the healthcare industry's needs and concerns is necessary.

4. **Clearly communicate tool policies, provide training sessions**
   To support adoption and mitigate shadow tool usage, policy communication must be widely disseminated and accessible in multiple locations for teams to reference. Additionally, users must clearly understand the reasoning for avoiding unsanctioned tools and the black box model—returning to core shared values of safety and security.

5. **Provide broader training on AI literacy**
   Training and educational sessions can help users clearly understand why it's critical to avoid unsanctioned AI tools that can introduce bias and impact patient safety. This is especially important as younger providers enter the workforce and haven't yet developed their professional clinical expertise to critically analyze AI outputs.

6. **Continue to monitor shadow tool presence, gathering feedback**
   Long-term adoption and success require staying updated on the latest tool features and workflow needs. It's crucial to maintain an open line of communication with providers on how AI tools are addressing—and not addressing—current challenges to stay ahead of potential unauthorized tool usage. Consider how this monitor and feedback step can inform AI policy refinement.

Despite the current tool alignment challenges, the excitement for AI solutions is palatable—the potential to search for information, analyze data, and improve care is engaging healthcare workers to search for tools that can solve current challenges.

When it comes to patient care, the stakes couldn't be higher for choosing the right tools. The value in AI lies in purpose-built solutions for healthcare enterprises that understand modern workflows, aim to solve for clinical and administrative challenges, and are mindful of the health, financial, and legal repercussions associated with incorrect responses or patient data breaches. With clear insight into organization-wide usage and trusted outputs for clinicians, health leaders can move confidently into the AI future with enterprise solution partners.

Explore how UpToDate supports enterprise-wide clinical decision-making with UpToDate Expert AI.

Learn more →

"As shadow AI continues to be more prevalent, clinicians should only use purpose-built GenAI systems that are trained on expert-validated evidence, transparent with source citations, and capable of tailored recommendations. GenAI will provide an increase in staff efficiency and care quality, but we must preserve safety and clinician-patient relationships by reframing workflows that elevate GenAI from a tool to a partner, keeping patients at the center of care."

Greg Samios, CEO,
Wolters Kluwer Health

References

1. Bruce, Giles. "Shadow AI goes 'mainstream' in healthcare: 5 notes." Becker's Health IT. December 18, 2025. https://www.becker-shospitalreview.com/healthcare-information-technology/ai/shadow-ai-goes-mainstream-in-healthcare-5-notes/
2. Online survey of hospital and health system providers and administrators conducted on behalf of Wolters Kluwer Health. N=518, comprised of 256 providers and 262 administrators. Conducted December 2025. Data on file.
3. Porter, Justin, et al. "Revisiting the Time Needed to Provide Adult Primary Care." Journal of General Internal Medicine. 38, 1. (2023): 147-155. doi:10.1007/s11606-022-07707-x
4. Jain, Sachin." AI Adoption In Healthcare Is Surging: What A New Report Reveals." Forbes. October 21, 2025. https://www.forbes.com/sites/sachinjain/2025/10/21/ai-adoption-in-healthcare-is-surging-what-a-new-report-reveals/
5. IBM. Cost of a Data Breach Report 2025. Accessed December 2025. https://www.ibm.com/reports/data-breach
6. Bonis, Peter. "Avoiding a future where the 'cause of death' is an AI chatbot." Chief Healthcare Executive. July 8, 2025. https://www.chiefhealthcareexecutive.com/view/avoiding-a-future-where-the-cause-of-death-is-an-ai-chatbot-viewpoint
7. Donnellan, Alison. "Engineering identity: Anonymous data remains vulnerable to re-identification through basic details." MSN. com. November 28, 2025. https://www.msn.com/en-us/technology/cybersecurity/engineering-identity-anonymous-data-remains-vulnerable-to-re-identification-through-basic-details/ar-AA1Rlrwz
8. American Medical Association. National physician burnout survey. May 15, 2025. https://www.ama-assn.org/practice-management/physician-health/national-physician-burnout-survey
9. North, Madeline. "7 ways AI is transforming healthcare." World Economic Forum. August 13, 2025. https://www.weforum.org/stories/2025/08/ai-transforming-global-health/
10. Krishna, Aneesh, et al. "The coming evolution of healthcare AI toward a modular architecture." McKinsey & Company. November 18, 2025. https://www.mckinsey.com/industries/healthcare/our-insights/the-coming-evolution-of-healthcare-ai-toward-a-modular-architecture