

The Agentic AI trust gap

Why healthcare needs
identity-led governance



Executive letter

Dear healthcare leaders,

Artificial intelligence is entering a new phase in healthcare.

Over the past several years, healthcare organizations have explored how AI can support clinical decision-making, reduce administrative burden, and make operations more efficient. Now, organizations are beginning to adopt agentic AI: systems that can reason through complex tasks, make decisions, and take action with varying degrees of autonomy.

There is a great deal of promise in that shift. Used responsibly, agentic AI has the potential to reduce friction in healthcare workflows and give clinicians more time to focus on patients. But as AI agents move from providing information to actually performing work, the stakes change.

An AI agent may be able to access sensitive data, interact with clinical and operational systems, or take action on behalf of a user or organization. That raises practical questions healthcare leaders need to answer before these technologies scale:

- **What systems and data should an AI agent be able to access?**
- **What actions should it be permitted to take?**
- **Who is accountable when an agent takes those actions?**
- **How do we know an agent is operating within its intended boundaries?**
- **And can we reliably monitor and audit its activity over time?**

These are not simply technical questions. In healthcare, decisions about access, authorization, and oversight can have real consequences for clinicians, operations, and ultimately patient care.

To better understand how organizations are preparing for this next stage of AI adoption, Imprivata commissioned independent research conducted by Vanson Bourne, surveying 250 U.S. healthcare leaders responsible for identity security and AI strategy.

The findings point to an industry moving quickly. They also reveal an important gap. Healthcare leaders are generally confident in their ability to govern AI agents, yet many acknowledge that existing governance practices are struggling to keep pace with rapidly expanding AI capabilities. In some cases, AI tools are already being used outside formal approval processes, making it harder for organizations to maintain visibility, accountability, and control.

That is why identity needs to be part of the foundation for agentic AI. An AI agent should be treated as a governable digital identity, with access appropriate to its role, clear limits on what it can do, and a record of its activity that can be monitored and audited.

Getting there will require more than a single security control. Organizations will need credential protection, least-privilege access, delegated authority, appropriate approval workflows, ongoing monitoring, and clear governance around how AI agents are provisioned and managed.

Healthcare should continue to move forward with AI. The opportunity is too important to ignore. But innovation and oversight have to advance together. The goal is not simply to enable AI agents to do more. It is to make sure they can do so safely, responsibly, and in ways that support the people delivering care.

I hope this report helps healthcare leaders identify where governance gaps are emerging, understand how identity practices will need to evolve, and take practical steps to prepare for what comes next.

Sincerely,



Dr. Sean Kelly

Chief Medical and Growth Officer and Sr. VP, Customer Strategy, Healthcare
Imprivata

Healthcare is entering a new AI chapter

Artificial intelligence has become an established part of healthcare operations. Organizations already use traditional AI to improve administrative efficiency, support cybersecurity operations, streamline revenue cycle management, assist with clinical documentation, and augment decision-making across a wide range of workflows.

Agentic AI represents the next stage of that evolution.

In 2026, many organizations are moving beyond AI assistants that merely respond to prompts toward AI agents capable of planning and executing work with varying degrees of autonomy. That shift has the potential to reshape both clinical and operational workflows.

The potential benefits are substantial. Healthcare's complexity, however, makes the safe deployment of these tools particularly challenging.

Confidence in AI is growing, but so are the governance challenges

AI agents may interact with electronic health records (EHRs), identity systems, clinical applications, medical devices, and other technologies that support patient care. As these agents become increasingly autonomous, organizations must ensure they are sufficiently controlled to prevent their use from harming rather than helping organizations and patients.

The survey findings reflect both the momentum behind agentic AI and the governance challenges that accompany it:

83%

of surveyed organizations have already deployed AI across select departments, or multiple use cases, and 28% have agentic AI in production and use

88%

expect AI agents to operate with at least some degree of autonomy across both operational and clinical workflows

57%

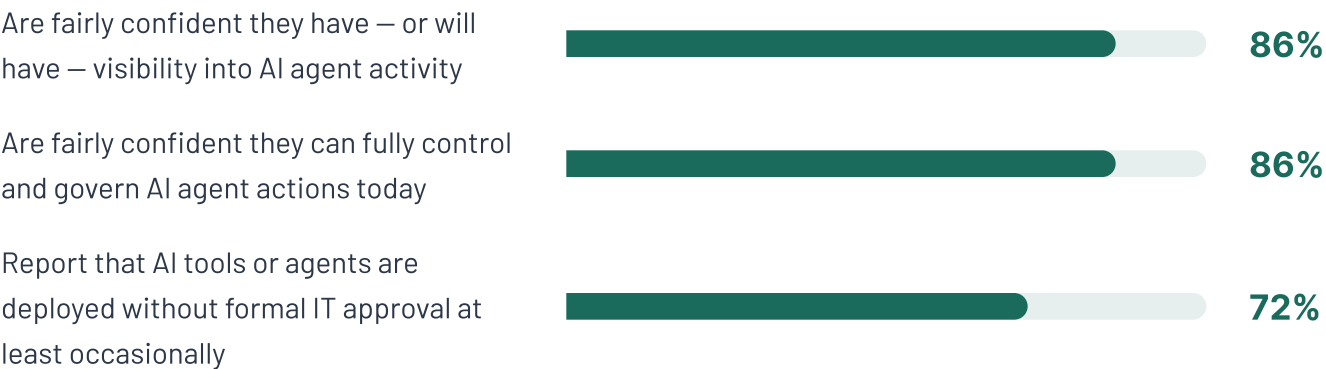
rank security among their top three concerns when planning or adopting agentic AI

For many healthcare organizations, the question is shifting from whether to adopt agentic AI to how to govern it responsibly. The concern is whether governance models can evolve quickly enough to support and control AI systems with the power to act on behalf of clinicians, staff, and the organization itself.

The readiness gap

The survey research also identifies a gap between organizational confidence and the reality of operational control. Most respondents express confidence that their organizations either have, or soon will have, the visibility and governance capabilities needed to manage AI agents effectively. At the same time, many acknowledge that the reach of AI tools and agents may already stretch beyond formal governance processes.

AMONG SURVEYED ORGANIZATIONS:



Organizations report using a variety of provisioning approaches, including centralized IT management, self-service platforms, and ad hoc implementation.

As agentic AI adoption accelerates, healthcare organizations need identity-led controls that make every AI agent visible, secured, monitored, and accountable throughout its lifecycle.

Research report roadmap

THIS REPORT EXAMINES:

- Where healthcare organizations are deploying agentic AI first
- Why access control, safeguarding protected health information (PHI), and auditability are foundational
- How organizations are redefining human oversight
- Why shadow AI exposes governance gaps
- How AI identity practices are evolving
- What healthcare organizations can do today to prepare for secure, scalable adoption

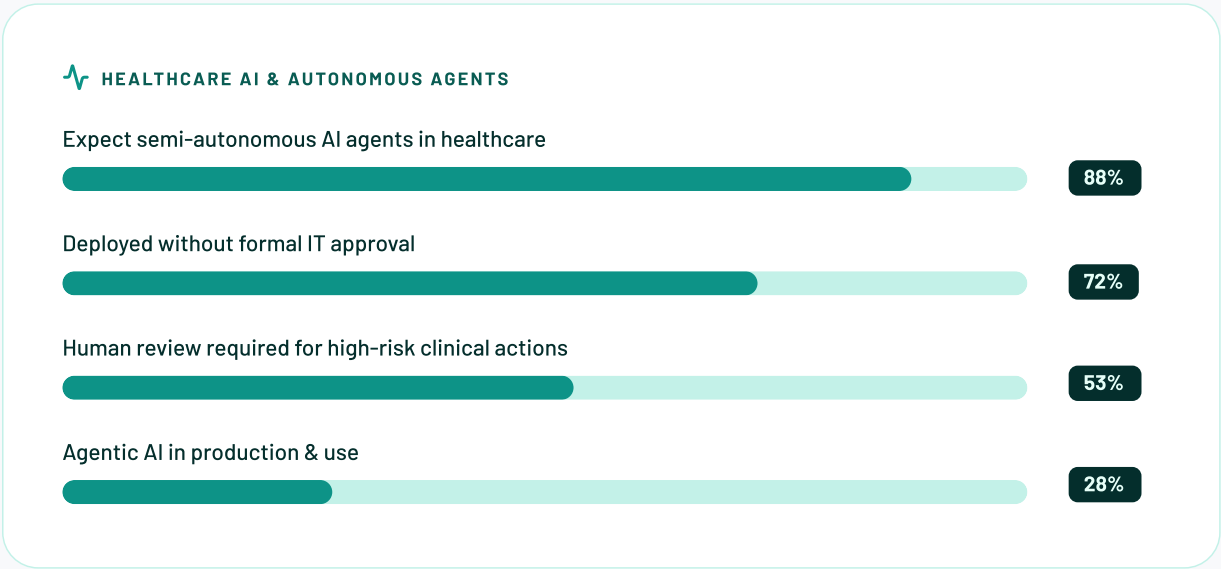
The research points to a clear conclusion. Healthcare organizations are moving quickly from AI experimentation toward agentic AI deployment. Governance, identity, access, and accountability models, however, are still evolving.

Agentic AI is moving from experimentation into live healthcare workflows

While AI adoption is widespread across the healthcare enterprise, agentic AI remains at an earlier stage of maturity. Many organizations are still evaluating where autonomous agents can deliver the greatest value, how much autonomy is appropriate for different use cases, and which governance models are needed to support broader deployment. Governance that appears centralized on paper may need stronger identity-based controls to make all agents visible, accountable, and secure.

Given that **83%** of surveyed organizations have already deployed AI across select departments or multiple use cases, it's clear that AI use in healthcare has moved well beyond experimentation. However, only **28%** of respondents report having agentic AI already in production and use, while **44%** are piloting or conducting proof-of-concept projects. Another **21%** expect to implement agentic AI within the next 12 months.

These findings point to an important inflection point. Over the coming year, many healthcare organizations are expected to transition from isolated pilot projects to broader deployments that span multiple departments and business functions. But all of these organizations are fully prepared for the potential risks these agents introduce.



"The existing identity recognition framework is mature, but it needs to be adapted and optimized for the automation behavior, dynamic permission adjustment, and traceability of AI agents to ensure security and controllability."

– Senior management, Integrated Delivery Network, 1,000+ beds

Agentic AI is beginning to reshape both clinical and operational work

Survey respondents estimate that agentic AI is currently involved to some degree in **33%** of clinical workflows and **37%** of operational workflows. Within the next 12 to 18 months, they expect those figures to increase to **41%** and **46%**, respectively.

Respondents also anticipate a significant organizational impact from these technologies. Nearly four in five (**79%**) expect agentic AI to have a transformative or significant impact on clinical workflows, and **73%** expect the same for operational workflows.

Operational workflows are presently leading adoption because AI agents can automate repetitive, lower-risk activities while organizations gain experience with governance and oversight. Clinical workflows, by comparison, require a higher degree of confidence because AI agents may interact with PHI, support clinical decisions, or participate in workflows that directly impact patient care and compliance.

The findings suggest that most healthcare leaders view agentic AI as more than another productivity tool. They see it as an operational capability that will influence how work is performed across the healthcare enterprise.

AI Deployment

83%

have deployed AI across select departments or multiple use cases

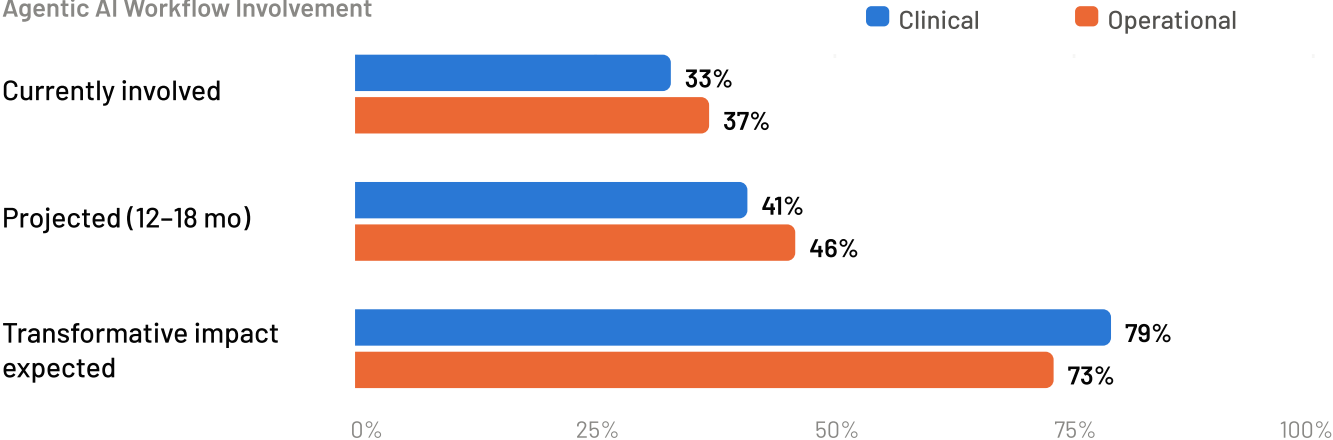


Agentic AI Adoption Stage



In production & use Piloting / proof-of-concept Planning (within 12 months)

Agentic AI Workflow Involvement





The challenge of agentic AI is not only capability, but also control

As agentic AI expands beyond isolated use cases, AI agents begin interacting with a wider range of applications, identities, and sensitive information. An AI agent supporting appointment scheduling presents a very different risk profile than one that retrieves patient records, assists with clinical documentation, or coordinates care across multiple systems. As organizations deploy larger numbers of agents across diverse workflows, governance becomes more complex.

The survey leaves little doubt that healthcare organizations see tremendous potential in agentic AI. At the same time, healthcare leaders must approach adoption with appropriate caution. As AI agents gain access to clinical systems, privileged applications, and PHI, AI agent security becomes as important as the technology itself.



Takeaway: As agentic AI expands from isolated workflows to broader operational and clinical use, identity becomes the foundation for scaling safely. Organizations need to ensure that each agent has only the access and authority required for its specific role, with activity continuously monitored as its permissions, workflows, and level of autonomy evolve.

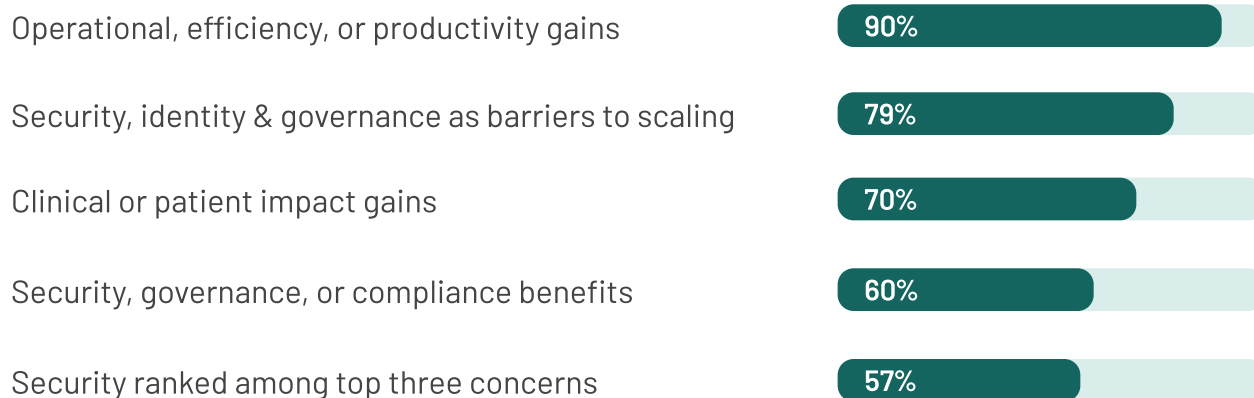


Organizations expect measurable value

Healthcare leaders expect agentic AI to deliver benefits across multiple dimensions of the enterprise.

Among surveyed organizations:

Agentic AI: Expectations & Concerns



These findings show that organizations view agentic AI as more than a tool for automation. Many see AI agents as a way to reduce administrative burden, improve resource utilization, strengthen operational resilience, and support clinicians in delivering care.

Realizing those benefits, however, depends on establishing confidence that AI agents will consistently operate within approved policies and intended boundaries.

Security remains the leading obstacle

While respondents are optimistic about agentic AI's potential, security concerns remain a major barrier to broader adoption. More than half rank security among their top three concerns when planning or adopting agentic AI, and **79%** identify security, identity, or governance issues as among the most significant barriers to scaling agentic AI.

The survey suggests that excessive access is emerging as a primary governance risk, with **57%** of respondents ranking excessive or unnecessary access permissions among their top concerns regarding agents that interact with clinical systems. This finding reflects an important shift in how healthcare organizations must think about security.

Unlike traditional software, AI agents may independently access multiple systems, retrieve sensitive information, invoke APIs, and execute workflows on behalf of users. Without clearly defined identity, authorization, and monitoring controls, organizations risk creating new pathways to excessive access, unintended actions, and compliance violations.

Stronger governance does not have to come at the expense of AI adoption. By establishing clear controls around agent identity, access, authorization, and monitoring, security and IT teams can evaluate AI workflows based on defined risk rather than relying on broad restrictions. This can give organizations greater confidence to enable appropriate AI use while maintaining the safeguards required for higher-risk workflows.

Healthcare leaders identified data security and regulatory compliance as significant concerns surrounding agentic AI. Nearly half of respondents cited unauthorized access to PHI and potential compliance or regulatory violations among their top concerns (**47.6%** and **49.6%**, respectively). These concerns were especially prominent among board and C-suite respondents: **64%** identified compliance or regulatory violations as a top-three concern, and **54%** viewed security risks as a barrier to scaling agentic AI. The findings suggest that senior leaders are considering not only technical risks, but also the wider accountability, regulatory, and patient-trust implications of AI-related incidents.



Autonomy requires guardrails



Clinicians are more likely to embrace AI efforts if the governance, supervision, and accountability frameworks are clearly explained."

– Board member/C-level; Single hospital; 250–499 beds

The survey also highlights an important tension between the desire for autonomous AI and the need for human oversight.

Historically, identity security focused primarily on verifying who or what could access a system. Applying least-privilege access becomes even more important as AI agents perform sophisticated work across clinical and operational environments. And as agentic AI becomes more autonomous, organizations must place equal emphasis on defining what an AI agent is authorized to do after access has been granted.

While **88%** of respondents expect AI agents to operate with at least some degree of autonomy across clinical and operational workflows, **53%** say human review is still required for high-risk clinical actions, and **40%** say the same for high-risk operational actions.

Lower-risk administrative activities may require little or no human intervention. Higher-risk activities — such as accessing PHI, supporting clinical decisions, or performing privileged actions — may require additional safeguards, including human approval, step-up authentication, or other governance controls.



Our hospital previously experienced an anomaly where AI automatically exported patient information in batches. We were only able to quickly pinpoint the risk thanks to audit logs. Therefore, we only dare to expand the deployment of AI once our monitoring system is mature."

Senior management; Health system/hospital system; 500–749 beds



Takeaway: As AI agents gain access to clinical systems and sensitive information, organizations must know who — or what — is acting, the type of access granted, what actions were taken, and whether those actions were authorized. Identity-aware governance provides the controls needed to answer those questions consistently while enabling organizations to scale agentic AI with confidence.

Healthcare wants autonomy, but not without accountability

Healthcare organizations are not resisting agentic AI. In fact, the survey suggests the opposite. Respondents overwhelmingly expect AI agents to become more capable and more autonomous over the coming years. The remaining questions concern where that autonomy is appropriate, where additional oversight is required, and how to prove accountability when an agent acts.

AI GOVERNANCE & HUMAN REVIEW



Board members and C-suite respondents are more likely than mid-level or junior managers to say human review is required for every action

Mandatory Oversight Guardrailed / Audited Autonomy





Healthcare leaders are not necessarily trying to keep humans involved in every AI-driven workflow. Instead, they are working to determine when human review is necessary, when exception-based governance is sufficient, and how to demonstrate accountability when an AI agent acts.

Rather than viewing autonomy as an all-or-nothing proposition, organizations are developing governance models that align oversight with risk levels. Routine administrative tasks may require little human intervention, while clinical workflows demand a higher threshold of trust because AI agents may access EHRs, retrieve PHI, support clinical decision-making, or initiate actions that directly impact patient care.

Operational workflows — including IT operations, cybersecurity, revenue cycle management, scheduling, and hospital administration — often provide opportunities for organizations to mature governance models before expanding autonomy into higher-risk clinical settings. While these workflows still require appropriate controls, organizations may be more comfortable allowing AI agents to operate with greater independence because errors are generally easier to identify and remediate before they affect patients.



Takeaway: Human-in-the-loop governance is not a single policy setting. As agentic AI becomes more capable, healthcare organizations are moving toward governance models that adjust oversight according to the level of risk. Building those models requires identity-aware controls that can determine who — or what — is acting, what authority has been delegated, what level of access is appropriate, and when additional human review or approval should be required.

Accountability becomes a shared responsibility

For agentic AI, greater autonomy should not mean less governance, but rather governance that adapts to the risk level associated with each workflow and action. Organizations with more mature AI programs increasingly require accountability to be shared across multiple teams.

As AI agents become embedded across organizations, distributing responsibility among executive leadership, cybersecurity, IT, legal and compliance, clinical leadership, and operational departments is essential. A simple AI agent supporting patient scheduling, for example, may interact with identity systems, EHRs, communications platforms, and revenue cycle applications within a single workflow.

As adoption expands, governance becomes an enterprise capability rather than solely an IT responsibility.

"Intelligent AI has the ability to execute autonomously, and without a governance framework, it is prone to unauthorized operations and compliance risks. Clear governance can unify rules and control risks, which is a prerequisite for large-scale implementation."

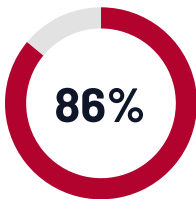
— Senior management; Single hospital; 500–749 beds

Healthcare leaders are confident in visibility, but unapproved AI is widespread

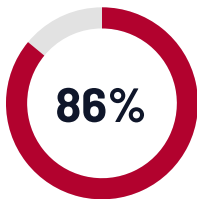
One of the most revealing findings in this research is the contrast between organizational confidence and operational reality.

Eighty-six percent of healthcare leaders are confident their organizations either have – or soon will have – visibility into AI agent activity, and 86% are also confident that they currently have the control needed to effectively govern AI agent actions. However, many acknowledge that AI tools and agents are already appearing outside of their formal governance processes, with 72% reporting that AI tools or agents are deployed without IT approval at least occasionally, 14% reporting known visibility gaps, and 37% citing an ad hoc or unapproved approach to AI agent provisioning.

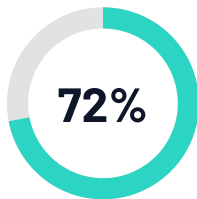
AI AGENT CONFIDENCE



Fairly confident they have (or will have) visibility into AI agent activity

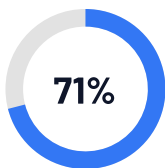


Fairly confident they can fully control & govern AI agent actions today

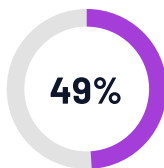


Report AI tools or agents are deployed without IT approval at least occasionally

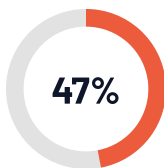
AI agent provisioning is fragmented, with many organizations using multiple different approaches:



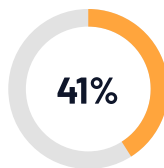
Centrally managed by IT



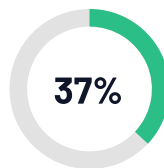
Managed by security



Self-service via approved tools



Decentralized departmental provisioning



Ad hoc or unapproved deployment

These findings are not mutually exclusive. Respondents could select multiple answers, reflecting the use of several provisioning models within the same organization.

While the fragmented approach reflects the current stage of AI adoption, it also introduces governance complexity. Different provisioning models often lead to inconsistent identity management, approval processes, and visibility into AI agent activity.



Ownership of governance is important, but not enough

The research also suggests that assigning responsibility for AI governance does not, by itself, ensure effective governance.

Even when organizations designate a Chief AI Officer, Chief Information Security Officer (CISO), Chief Information Officer (CIO), or governance committee to oversee AI strategy, AI agents can still emerge outside formal approval processes. In fact, 73% of organizations that have a Chief AI Officer overseeing AI strategy report AI tools being deployed without formal IT or security approval, as do 54% with CIO oversight, and 44% with CISO oversight.

This does not necessarily indicate widespread disregard for compliance regulations. Organizations with dedicated AI or security leadership may have greater visibility into unauthorized agents that would otherwise remain undetected. They may also operate more mature or complex AI environments. But more broadly, the prevalence of shadow AI agents in these organizations reflects the increasing accessibility of AI technologies.

Departments can evaluate AI-enabled applications independently, users can experiment with publicly available AI services, and software vendors continue embedding AI capabilities into existing platforms. As a result, organizations may have formal governance policies while still struggling to maintain visibility into how AI is actually being used throughout the enterprise.

These findings reinforce that governance requires more than organizational ownership. It requires safeguards that ensure every AI agent can be discovered, attributed, monitored, and controlled regardless of where it originates.

Visibility must extend to every AI agent

As healthcare organizations expand their use of agentic AI, visibility must extend beyond human users to include every AI agent or other non-human identity operating across the environment.

Organizations need to answer fundamental questions such as:

- Which AI agents currently exist across the enterprise?
- What systems and data can they access?
- Who owns or sponsors each agent?
- What authority has been delegated to them?
- What actions can/have they performed?
- Can those actions be reconstructed during an audit?

Answering these questions becomes more difficult with inconsistent provisioning practices, or when AI agents rely on fragmented identity and access mechanisms, including shared service accounts, delegated clinician authority, embedded credentials, and API keys.

Shadow AI makes these challenges even more urgent by introducing AI agents that may operate outside established governance processes.



Takeaway: AI governance cannot rely on organizational ownership alone. As agentic AI adoption accelerates, healthcare organizations need practical identity and access controls that make every AI agent discoverable, attributable, appropriately permissioned, continuously monitored, and fully governable throughout its lifecycle.

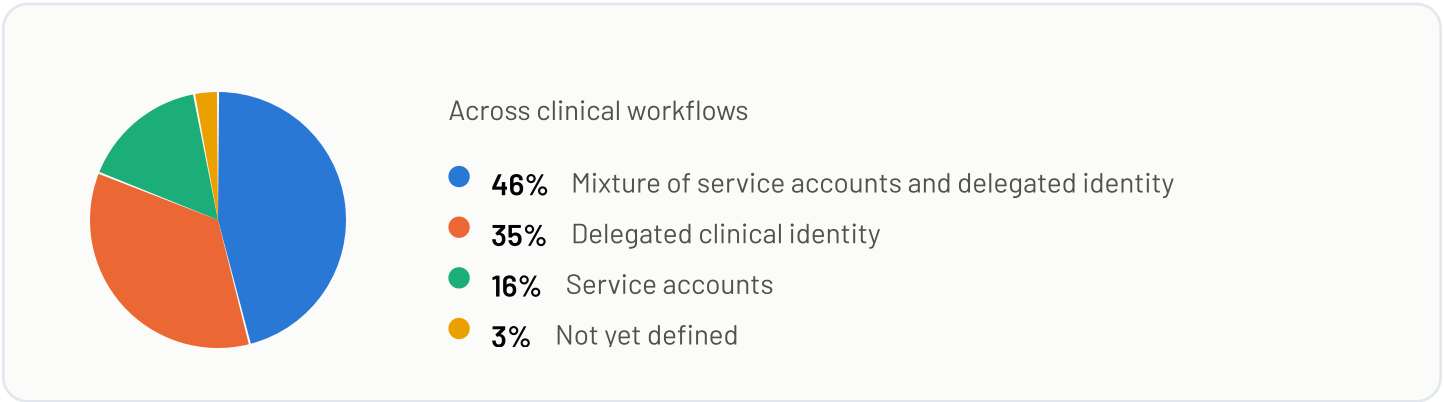
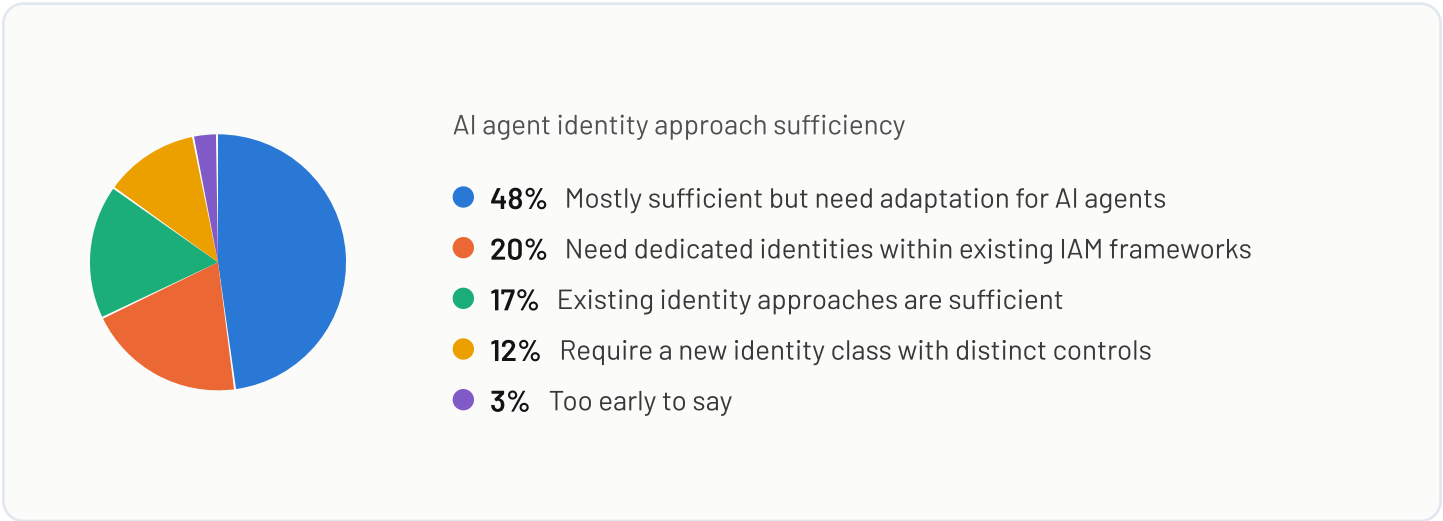
Healthcare organizations know AI agents need identity, but approaches remain fragmented

As healthcare organizations expand their use of agentic AI, one question is becoming increasingly important: What exactly is an AI agent from an identity perspective?

The survey suggests there is not yet a consensus. Some organizations believe existing identity and access management (IAM) frameworks can be adapted to support AI agents. Others believe agents require dedicated identities with their own lifecycle and governance controls. Still others view agentic AI as introducing an entirely new class of digital identity.

The lack of agreement is understandable. Traditional identity models were designed primarily for people, applications, and service accounts, not autonomous software capable of making decisions, initiating workflows, and acting on behalf of clinicians or employees.

How AI Agents Authenticate



The lack of standardization around AI agent identity creates risk, but it also creates an opportunity for healthcare organizations, standards bodies, and trusted technology partners to establish practical governance models and define best practices.

Identity governance must evolve for AI agents

Agentic AI introduces governance requirements that traditional identity models were not designed to address. Unlike conventional software, AI agents can plan, initiate multistep workflows, invoke tools dynamically, and act under delegated human or organizational authority.

Delegated authority requires explicit governance, particularly in clinical workflows. Because AI agents can act independently and at machine speed, organizations must clearly define the scope of an agent's authority rather than relying on implicit assumptions.

Using shared or opaque service accounts for AI agents may simplify implementation, but can make it difficult to determine which agent performed a particular action or under whose authority it acted. Hybrid identity approaches offer flexibility but can also increase operational complexity when identity policies are inconsistently applied across environments.

Healthcare organizations need policies that answer questions such as:

- Which actions may an AI agent perform independently?
- Which actions require clinician approval?
- When should step-up authentication be required?
- Under whose authority is the agent operating?
- When does delegated authority expire?
- What data may the agent access or disclose?
- Which tools or downstream agents may it invoke?
- How is the agent's identity created, changed, suspended, and retired?
- What happens when the agent behaves outside expected parameters?

"We need a dedicated identity class for AI agents because they operate autonomously and continuously access sensitive systems, requiring distinct authentication, least-privilege authorization, and full audit trails to ensure security, accountability, and compliance."

– Senior management; Specialty hospital; 500–749 beds

Dedicated AI agent identities forge a clearer path to accountable governance. Unique identities make AI activity attributable and auditable, and enable organizations to define authorization policies, enforce least-privilege access, manage identity lifecycles, monitor behavior, and maintain comprehensive audit trails.

These capabilities become increasingly important as organizations potentially move from managing dozens of AI agents to hundreds — or eventually thousands — operating across clinical and operational environments.

Every AI agent should operate within clearly defined identity and access rules that align permissions with its specific workflow, the sensitivity of the data being accessed, the level of risk involved, and the degree of autonomy granted. Auditability should be built into every AI-driven action from the outset so organizations can demonstrate accountability, support regulatory compliance, and maintain trust as AI adoption expands.

Takeaway: Agentic AI introduces a new class of digital identity. Healthcare needs governance models that account for what agents are, who they act for, what they can access, and how their actions are reviewed.

Safeguarding healthcare organizations through the next phase of AI adoption

The survey findings point to rapid advancement from AI experimentation toward operational use of agentic AI across healthcare organizations. The next challenge is determining how to scale autonomous AI safely while maintaining the privacy and trust that healthcare demands.

Security and governance remain among the leading barriers to broader adoption. Organizations express concern about excessive permissions, PHI exposure, compliance risk, and limited auditability, particularly as respondents expect AI agents to become more autonomous over the coming years.

AI agent identity is emerging as a crucial aspect of healthcare security. Existing IAM approaches will need to evolve to support agent identity, delegated authority, least-privilege access, continuous monitoring, and audit-ready accountability.

Next steps: Five foundational actions for scaling agentic AI safely

- 1 Inventory where AI agents are already operating**
Including each agent's owner, purpose, deployment status, connected systems, and source.
- 2 Assign every agent a governable identity**
Manage that identity from provisioning through decommissioning. Avoid shared or opaque accounts that prevent independent attribution.
- 3 Apply least-privilege access by workflow and risk level**
Agent permissions should reflect the task, system, data sensitivity, and level of autonomy. Permissions should be time-bound and context-aware when warranted by risk level.
- 4 Define when human approval or step-up is required**
Especially for PHI access, order entry, clinical decision support, privileged actions, and high-risk operational workflows.
- 5 Build auditability into every AI-driven action**
Healthcare organizations should be able to demonstrate what every AI agent did, under whose authority it acted, what systems it accessed, and whether its actions were authorized and consistent with policy.

"Medical institutions have extremely high information security requirements, and strong security controls can ensure that the access and operation of AI agents are traceable throughout the entire process, meeting regulatory compliance requirements."

— **Junior management; Health system/hospital system; 500–749 beds**



Questions every healthcare leader should ask

Agentic AI may help healthcare organizations improve efficiency, productivity, and aspects of patient experience, but only if agents are governed with rigor appropriate to their access, autonomy, and potential impact.

As organizations prepare for broader adoption of agentic AI, leadership teams should consider several fundamental questions:

- Are we enabling AI innovation without compromising security, trust, or regulatory compliance?
- Is our governance model prepared to manage autonomous AI agents?
- Under whose authority is each AI agent acting?
- Can we revoke or constrain an agent's authority quickly?
- How will we demonstrate accountability for every AI-driven action?

Organizations that can answer these questions with evidence will be better positioned to responsibly scale agentic AI.

Imprivata helps healthcare organizations secure every identity, human and non-human, so they can accelerate innovation without sacrificing control, compliance, or trust.

Learn more about [Imprivata Agentic Identity Management](#) and how we can help support secure AI agent adoption.

Methodology

Survey conducted by Vanson Bourne for Imprivata.

250 healthcare leaders with responsibility for identity security and/or AI strategy from U.S. public and private healthcare organizations, including IDNs, hospital systems, single hospitals, academic medical centers, and specialty hospitals, responded to the survey.

Healthcare Organization Type

Organization Type	Respondents	%
Health system / hospital system	74	29.6%
Integrated Delivery Network (IDN)	55	22.0%
Single hospital	55	22.0%
Academic medical center	35	14.0%
Specialty hospital	31	12.4%

Organization Size (Patient Beds)

Bed Count	Respondents	%
100–249 beds	15	6.0%
250–499 beds	54	21.6%
500–749 beds	104	41.6%
750–999 beds	49	19.6%
1,000+ beds	28	11.2%

Professional Seniority

Position Level	Respondents	%
Board member / C-level	39	15.6%
Senior management	105	42.0%
Mid-level management	86	34.4%
Junior management / frontline supervisors	20	8.0%



Imprivata delivers access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. Imprivata's platform of innovative, interoperable access management and privileged access security solutions enable organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership. For more information, visit www.imprivata.com

Global headquarters USA

Waltham, MA

Phone: +1 877 663 7446

www.imprivata.com

European headquarters

Uxbridge, England

Phone: +44 (0) 208 744 6500

www.imprivata.com/uk

Germany

Langenfeld

Phone: +49 (0) 2173 99 385 0

www.imprivata.com/de

Australia

Melbourne

Phone: +613 8844 5533



Copyright © 2026 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.