

Closing the AI Governance Gap

What the 2026 Healthcare Benchmark Means
for Your Organization

Thursday, October 22

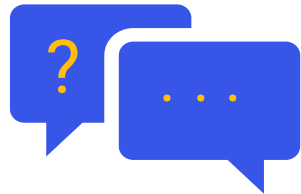


Meeting Logistics



Microphones

All attendees are on mute.



Questions

Type your questions in the Q&A box.



Resources

Upcoming events & resources linked.



Recording

Recording will be provided after event.



Survey

Survey will prompt at the end of the session.

Your Presenters



Harry Lu

VP, Consulting Services - AI Solutions

- Experience in helping organizations of different sizes securely adopt AI technologies, advising client executives on matters ranging from strategy through execution
- Experience in researching and developing cutting edge AI security solutions
- Experience working with organizations in healthcare industry, including care providers, payers, and technology providers
- Master of Science in Information Systems, University of Maryland - College Park

<https://www.linkedin.com/in/harry-lu-53aaa138/>

Who we surveyed and what we asked

Beyond whether an artificial intelligence (AI) policy exists, we asked what organizations can see, control, verify, and prove.

105

organizations surveyed,
late July through early
September 2026

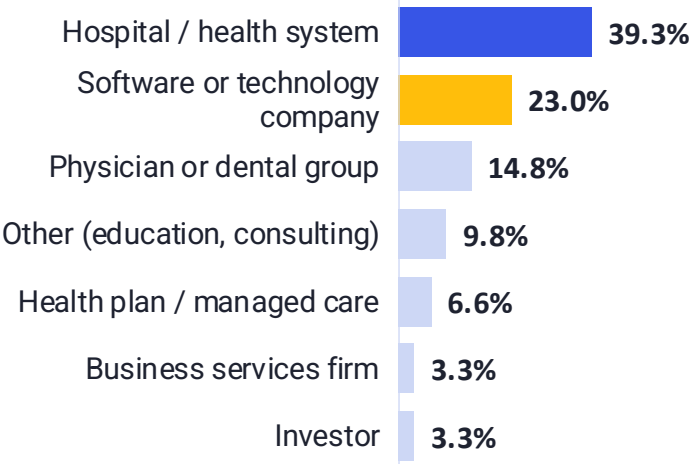
WHAT WE ASKED

Inventory: is AI verified against what is actually running?

Data: is movement into AI services controlled?

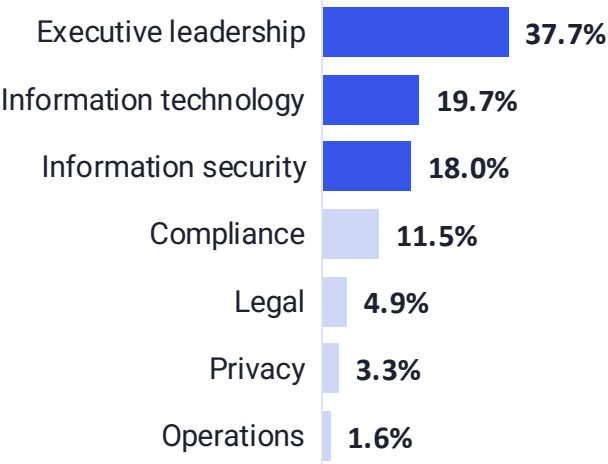
Vendor: are vendor AI controls verified?

ORGANIZATION TYPE



Gold: software and technology companies, the second-largest group. Organization type reflects respondents who identified one.

FUNCTIONAL ROLE



HOW TO READ THE DATA

Results represent a directional industry benchmark rather than a statistically representative measure of the healthcare sector. Treat 2026 as the baseline. Clearwater will ask the same questions again in 2027.

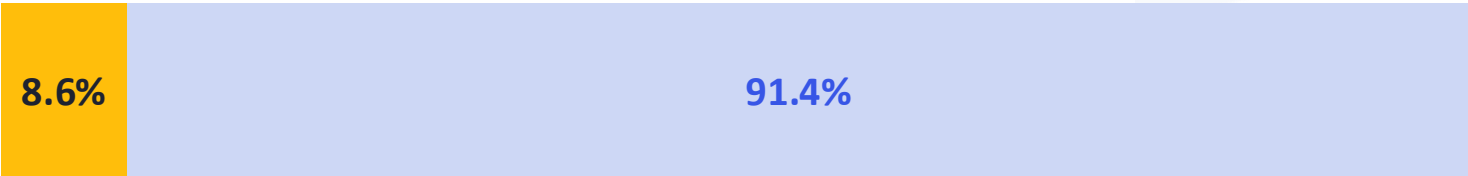
Source: Clearwater 2026 Healthcare AI Security and Governance Benchmark, pages 10 and 16, and the benchmark summary.

Only 8.6% can verify what AI is actually running

Organizations can count the artificial intelligence (AI) they believe they have. 91.4% cannot validate that count.

8.6%

validate their AI inventory
through automated discovery



Validated through automated discovery

Rely on a manual list, an unvalidated inventory, or no inventory at all

WHY IT MATTERS

30.8%

name unapproved employee AI use as their greatest AI-related data risk

42.3%

name sensitive data exposure through AI tools as a leading concern

CLEARWATER'S INSIGHT

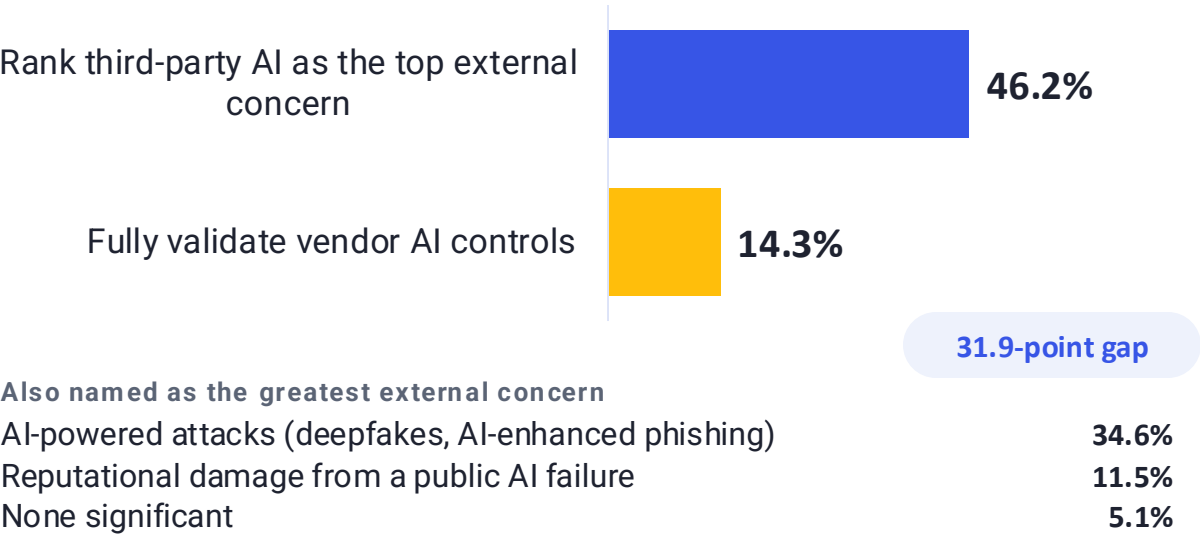
When we compare automated discovery with a client's approved AI list, the two rarely match. The list is rarely wrong. The environment simply changed faster than the list did, which makes inventory a continuous monitoring function rather than a documentation exercise.

Source: Clearwater 2026 Healthcare AI Security and Governance Benchmark, page 7.

Third-party AI is the top concern and the least verified

Most organizations inherit AI from third parties, but only 14.3% fully validate those controls.

CONCERN VERSUS VERIFICATION



WHAT A QUESTIONNAIRE CANNOT CATCH

- AI functionality added after contract signature
- Subprocessors and external foundation models
- Prompt and output retention
- Agents granted standing access to clinical systems
- Model changes shipped as routine updates

None of that requires a new contract, so none of it reliably triggers a new review.

CLEARWATER’S INSIGHT

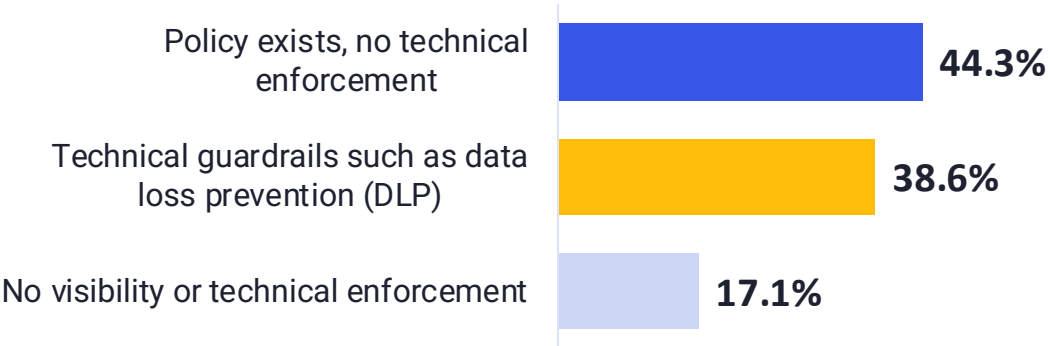
A security questionnaire is a point-in-time attestation. The AI behind a vendor relationship is not a point-in-time fact. Closing the gap takes a standing right to verify how vendor AI handles data, backed by technical evidence and refreshed on a regular cadence.

Source: Clearwater 2026 Healthcare AI Security and Governance Benchmark, page 9.

The most common control is a document

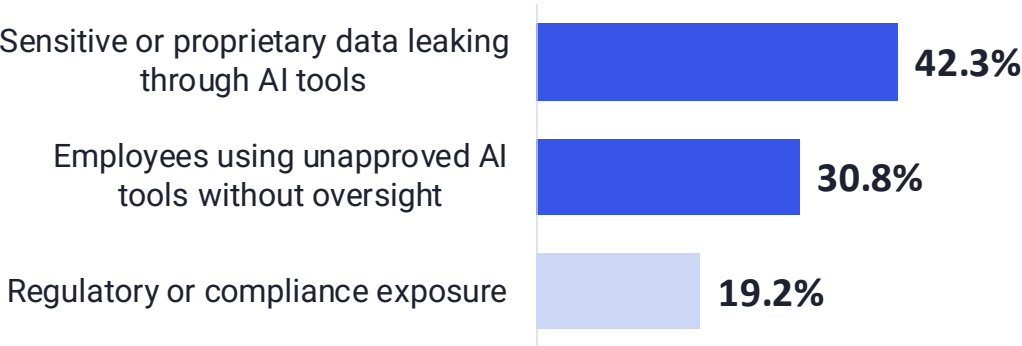
Nearly half rely on policy alone. Only 38.6% enforce data protection technically.

CONTROL POSTURE



44.3% report a policy with no technical enforcement, against 38.6% with technical guardrails

GREATEST INTERNAL CONCERN



73.1% name data leakage or shadow AI as their single greatest concern

WHAT A POLICY CANNOT DO

A policy can establish intent and accountability. It cannot detect an upload, block a paste, inspect a prompt, or show what is left after the fact.

“A, B, and C, all three, keep me up at night.”

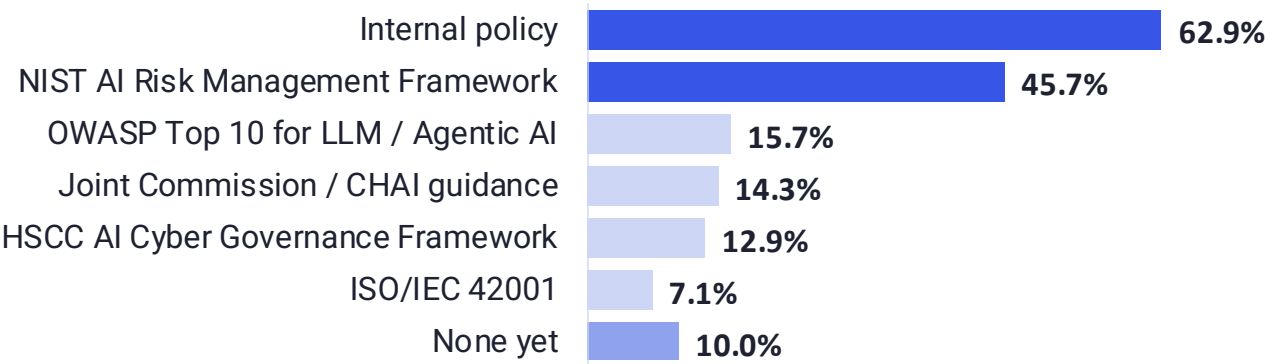
Anonymous survey respondent

Source: Clearwater 2026 Healthcare AI Security and Governance Benchmark, page 8.

Awareness is expanding. AI security controls remain thin

Internal policy guides 62.9% of organizations. Only 20.0% have adopted dedicated AI security technology.

GUIDING FRAMEWORKS (SELECT ALL THAT APPLY)



Lavender bars are AI-specific frameworks, none above 15.7%. NIST: National Institute of Standards and Technology. OWASP: Open Worldwide Application Security Project. LLM: large language model. CHAI: Coalition for Health AI. HSCC: Health Sector Coordinating Council. ISO/IEC: International Organization for Standardization and International Electrotechnical Commission.

TECHNOLOGY POSTURE



JUNE 2026

On June 1, 2026, the Joint Commission launched its Responsible Use of Artificial Intelligence in Healthcare certification. It asks organizations to demonstrate. That is the same word this study has been measuring.

CLEARWATER'S INSIGHT

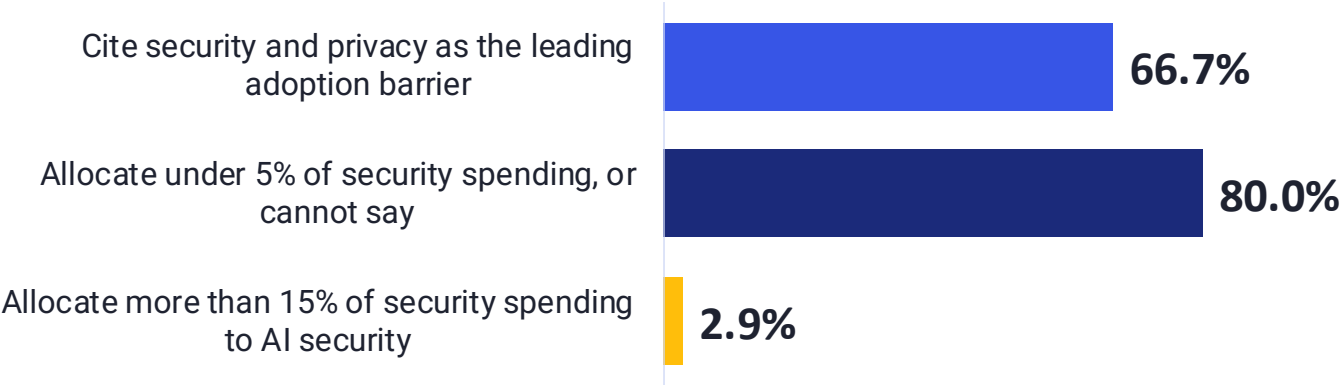
Healthcare organizations should not wait for one framework to emerge as the definitive standard. Choose a credible, security-specific AI framework now and use it to build a control structure the organization can actually operate, then test whether those controls work.

Source: Clearwater 2026 Healthcare AI Security and Governance Benchmark, page 12.

Security is the leading adoption barrier and the least funded

Security and privacy lead the adoption barriers at 66.7%. Four in five fund AI security below 5% or cannot say.

CONCERN AND SPENDING, SIDE BY SIDE



The 80.0% is 51.4% who allocate under 5% of annual security spending and 28.6% who do not know what they allocate.

WHY THE GAP EXISTS

- 1

No scoped plan of execution

“We’re concerned about this” never becomes a scoped set of controls with a cost attached.
- 2

Investment follows adoption

Licensing, integration, and new capability get funded. Protection is treated as a line item to revisit later.

CLEARWATER’S INSIGHT

Closing the gap does not require rebuilding the security budget. It requires a defined AI security workstream with its own scope, ownership, and funding, rather than leaving it buried inside the broader security program.

Source: Clearwater 2026 Healthcare AI Security and Governance Benchmark, page 11.

Closing the AI Governance Gap

Healthcare organizations have documented more AI governance than they can verify.

GAP ONE: THE INVENTORY

91%

of healthcare organizations cannot verify the AI running in their own environment.

GAP THREE: THE VENDOR

46%

name third-party AI as their top external concern, yet just 14% fully validate vendor controls.

THE INVESTMENT GAP

66%

cite security as their leading barrier to AI adoption, yet 80% underfund it.

Read the Full Report

See where your organization stands against the 2026 industry benchmark, including a three-question self-assessment to score your own gap.

[Download the Report](#)



Scan to download

A graphic consisting of four stylized human figures in a circle, holding hands, with the text "Q&A" in the center.

Q&A

Upcoming Virtual Events



- Next session November 5th @ 12 pm CT
- **Dave Bailey, VP of Consulting Solutions & Strategy, Clearwater:** Co-author of the HSCC's *Playbook for AI Clinical Resilience*, sharing guidance on AI risks in clinical workflows and the latest healthcare cybersecurity developments.
- **Dr. Benoit Desjardins:** An international leader in cardiovascular imaging, AI, and cybersecurity, joining the discussion on preparing for AI disruptions and protecting patient care.
- [Register here](#)

Upcoming In-Person Events



- November 11-14 | Denver, CO
- Hosting a focus group
- Sponsoring a top golf bay
- [Learn more + book a meeting](#)



- November 15-18, Las Vegas, NV
- CW Sponsoring the DHHF Digital Health & AI Awards
- 2 speaking sessions
- Meet us in the MATTER and DHHF Pavilions
- [Learn more + book a meeting](#)



- November 17, Las Vegas, NV
- Clearwater President Baxter Lee will speak at the Together.Health Partner Program at HLTH 2026 on Tuesday, November 17.
- [Learn more + book a meeting](#)



We are here to help.

*Moving healthcare organizations to a
more secure, compliant, and resilient
state so they can achieve their
mission.*



Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | [linkedin.com/company/clearwater-security-llc/](https://www.linkedin.com/company/clearwater-security-llc/)



Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Security & Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.