credo ai

Healthcare Edition · Report

The State of AI Governance in Healthcare

What 371 enterprise leaders reveal about the gap your organization needs to close.

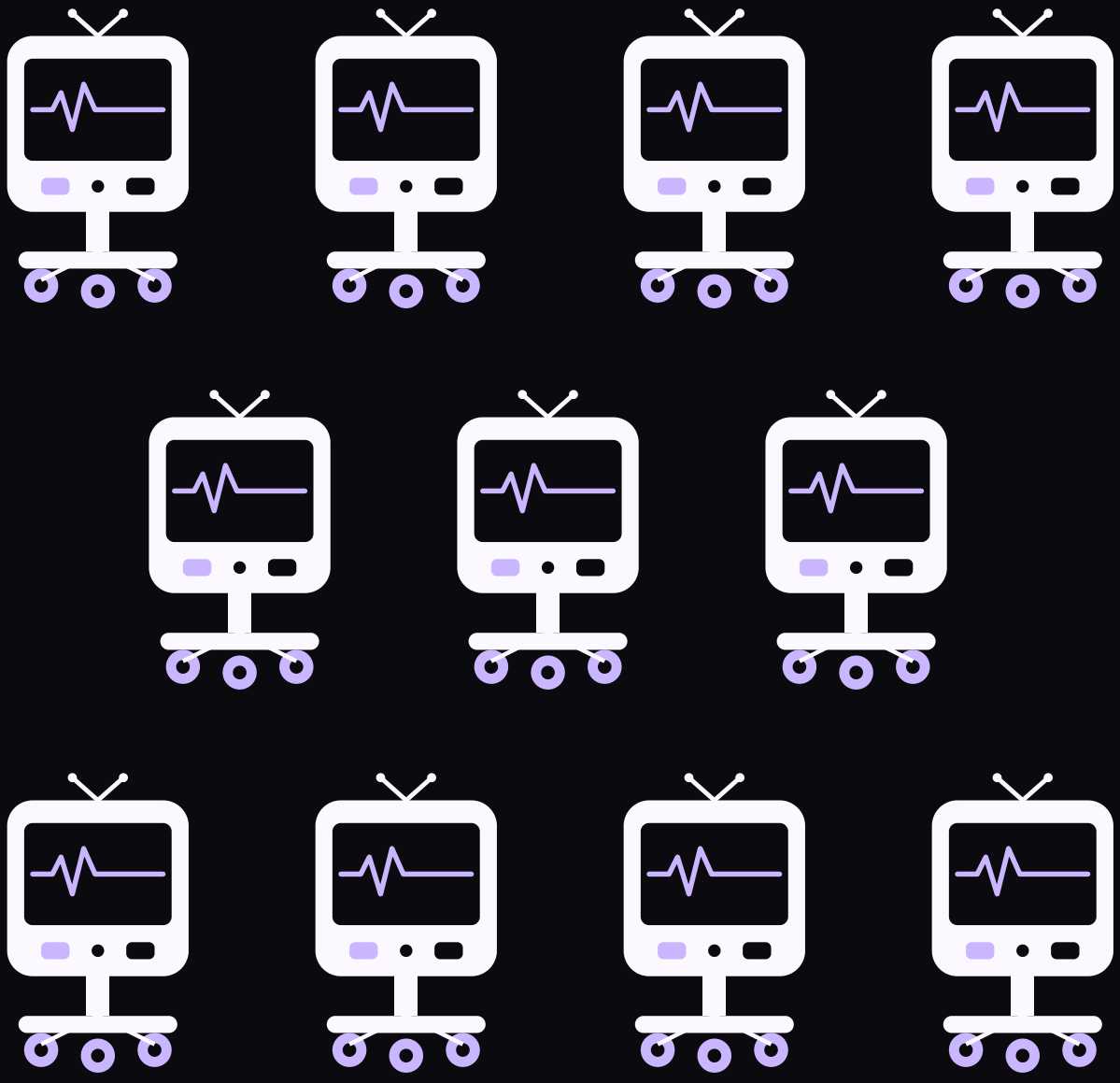

Table of contents

A NOTE ON THIS EDITION

Every stat in this report comes from a survey of 371 senior leaders across large enterprises. We've re-contextualized each finding for healthcare AI directors, CISOs, and chief data & AI officers operationally, not in the abstract.

• Executive Summary

Healthcare AI has crossed the threshold. But governance hasn't kept up.

Your clinical AI is in production. Your revenue cycle AI is running. Your ambient documentation tool is in every exam room. But if an auditor asked you today to show documented oversight for each one, where would you look?

SIX FINDINGS, HEALTHCARE-CONTEXTUALIZED

60%+

of enterprises deploy AI across multiple departments or company-wide. Most large health systems and payers have already crossed this line.

61% → 89%

Governance urgency jumps as AI moves from 1–2 departments to multiple. Healthcare is squarely past this threshold.

12%

of organizations use a dedicated AI governance platform. The other 88% rely on SharePoint, spreadsheets, and email-circulated Word docs.

45%

of teams lose 11–20 hrs/week to manual governance intake. At scale, that climbs to 21–40+ hrs for 27% of large enterprises.

41%

cite third-party AI risk as their hardest governance challenge. The most acute, least-solved pain point in healthcare.

3 hrs

to evaluate a single AI vendor. Mid-size health systems now manage 20+ AI vendor relationships, with no standardized scorecard.

88%

THE OPERATIONAL GAP

of healthcare organizations are governing AI today without a dedicated platform, using tools that can't produce the evidence HIPAA, The Joint Commission, and CMS 0057-F demand.

• Methodology

Healthcare-specific guidance, grounded in enterprise-scale data.

Every stat is sourced from **The State of AI Governance**, a survey of 371 senior leaders fielded November 2025. We've re-contextualized each finding for healthcare AI directors, CISOs, compliance leaders, and chief data & AI officers.

INDUSTRY SECTOR

Technology	38%
Financial services	29%
Healthcare & life sciences	14%
Manufacturing & retail	11%
Energy & infrastructure	5%
Government / defense	3%

ROLE / FUNCTION

CIO / IT leadership	26%
AI governance / risk	22%
Security / compliance	18%
Data / AI / ML	17%
Legal / procurement	10%
Other executive	7%

WHY A HEALTHCARE EDITION

Healthcare AI leaders repeatedly tell us: generic enterprise stats with a stethoscope icon are *not* what they need. The frameworks driving urgency are different (HIPAA, Joint Commission, CMS 0057-F, EU AI Act). The use cases are different (clinical decision support, prior auth, ambient documentation, vendor AI). The risk profile is different (PHI exposure, patient safety, clinical liability). **This edition reframes every finding through those realities.**

371
senior leaders surveyed

14%
healthcare & life sciences

81%
at orgs >1,000 employees

FINDING 01

Healthcare AI has crossed the threshold, AI governance hasn't kept up.

When AI moves from 1–2 departments to multiple, governance urgency jumps from 61% to 89%. Most large health systems and payers have already crossed this line.

60%+ of enterprises now deploy AI across multiple departments or company-wide. In healthcare, this means organizations are simultaneously running clinical decision support, revenue cycle AI, ambient documentation, prior authorization automation, and vendor-embedded AI features, each with different ownership, risk profiles, and regulatory obligations.

This is the threshold moment. The governance question has shifted from *"should we have a framework?"* to *"why can't we operate the one we have?"*

Only **12%** of organizations use a dedicated AI governance platform. The other 88% are governing AI with SharePoints, spreadsheets, manual review committees, and email-circulated documents.

HEALTHCARE AI IN PRODUCTION TODAY

- Clinical decision support
- Ambient documentation
- Prior authorization
- Revenue cycle AI
- Diagnostic imaging
- Vendor-embedded AI
- Care management
- GenAI assistants

EACH WITH ITS OWN REGULATORY EXPOSURE

- HIPAA audit
- Joint Commission
- CMS 0057-F
- HITRUST
- EU AI Act
- FDA SaMD

GOVERNANCE URGENCY BY AI ADOPTION STAGE

45%	61%	89%	92%
Pilots / pre-deployment	1–2 clinical or ops tools	**Multi-dept (clinical + ops)**	System-wide deployment

61% → 89% The step-change in urgency as AI expands from 1–2 departments to multiple parts of the organization. **Most healthcare systems are already past this point.**

• The compliance dimension

This gap isn't operational. It's regulatory.

HIPAA's audit requirements, The Joint Commission's clinical AI standards, ISO 42001's management system obligations, and the EU AI Act's high-risk provisions all require documented, continuous oversight. Manual processes can't produce the evidence these frameworks demand.

FRAMEWORK LENS

What auditors will ask for

Joint Commission
Documented oversight for any AI influencing clinical decisions, with bias and performance evidence on file.

HIPAA
Risk assessment and audit trail for every AI system that touches PHI, including vendor systems under a BAA.

ISO 42001 / HITRUST
Management-system evidence: documented roles, controls, and continuous monitoring, not point-in-time review.

EU AI Act
High-risk classification for medical AI; conformity assessments, post-market monitoring, and human oversight records.

CMS 0057-F
A documented inventory of every AI system in the prior authorization workflow, evidence of ongoing monitoring in production, and formal oversight of vendor AI operating on the payer's behalf.

88%

of organizations are governing AI without a dedicated platform.

> *"We've got AI features going into products. There's some in production, some in early access, a lot being discussed. It's a bit of a free for all at this moment in time." — AI Governance Lead, large healthcare payer*

WHAT THIS MEANS FOR YOU

The governance maturity required of healthcare organizations isn't growing linearly with AI adoption, it's growing faster. Every new clinical AI tool, every vendor AI feature, every shadow LLM in use multiplies the surface area you're accountable for documenting.

FINDING 02

The manual governance trap. What it costs healthcare teams.

45% of governance teams spend 11–20 hours per week on manual workflows. At scale, that climbs to 21–40+ hours. None of those hours are being spent on strategy.

45%

of governance teams spend 11–20 hrs/week on manual governance intake.

5% → 23%

share of teams burning 21–40 hrs/week as AI deployment scales from 1–2 systems to enterprise-wide.

30%

of high-risk AI use cases take ≥1 month to complete review. Low-risk cases stall in the same queue.

WHERE THE HOURS GO

For a healthcare AI director or program manager who owns governance as an *additive* responsibility, not a dedicated role, these hours aren't being spent on strategy. They're being spent on:

- **Chasing documentation** across SharePoint sites, team drives, and forgotten email threads.
- **Triaging use case requests manually** with no risk tiering. Every request gets the same intake form.
- **Running full reviews on low-risk tools** because the framework can't differentiate a meeting summarizer from clinical decision support.
- **Vetting third-party AI vendors one by one** without a standardized scorecard, reusable artifacts, or shared inventory.
- **Rebuilding context for every stakeholder** when legal, privacy, or security needs to be re-briefed on a review already in flight.
- **Pilot purgatory** AI programs pass technical validation, then stall in the governance queue for months.

> *"Team members have lost their appetite for the solution by the time the approval process has been completed." — AI Governance Director, large healthcare payer*

• The acute pain point

When Healthcare organizations buy, the math breaks fast.

A significant share of AI governance in healthcare isn't governing internal models, it's evaluating AI features embedded in vendor products.

THE VENDOR MATH

20+ AI vendor relationships at a typical mid-size health system

× 3 hrs to evaluate a single vendor manually, per discovery interviews

= 60+ hrs

per year on vendor triage as tools are updated or onboarded with no standardized methodology and no reusable artifacts.

TOOLING IN USE TODAY

Dedicated AI governance platform	12%
Hybrid (internal + 3rd-party tools)	39%
Primarily internal tooling	22%
Primarily manual processes	27%

ACTIVE MARKET SIGNAL

Multiple healthcare organizations are currently replacing or sunsetting OneTrust for AI governance, a tool originally built for privacy management, now generating more documentation burden than it relieves. The repurposed-tool era is ending.

> *"We're certainly struggling with both understanding what's in our contracts and what we can do in products, especially with data sharing." — AI Governance Director, regional health system*

FINDING 03

The capabilities healthcare AI leaders say they need most.

When 371 senior leaders rated AI governance capabilities, the priorities aligned. Here is each capability's market priority, plus what it actually means in a healthcare operating environment.

CAPABILITY	% RATED CRITICAL	WHAT IT MEANS IN HEALTHCARE
AI risk management Top priority across all roles	79%	Risk classification for clinical tools, PHI-handling AI, and vendor systems under HIPAA and Joint Commission obligations. Not a governance concept, a regulatory requirement.
Data governance visibility Foundational capability	76%	Knowing which AI systems access PHI, how it's being used, and whether BAAs are current. The first question every internal audit asks.
Shadow AI discovery Emerging priority	66%	Clinicians adopting ambient documentation, diagnostic aids, and consumer LLMs outside formal review. Healthcare-specific acute risk: rational behavior creating unmanaged PHI exposure.
Agentic AI observability Next frontier	65%	Autonomous AI making recommendations or taking action in prior auth, care management, and revenue cycle. Continuous observability isn't optional, it's what makes them governable.

Risk management is a regulatory obligation

HIPAA, Joint Commission, and the EU AI Act require risk assessments that **differentiate clinical AI from administrative AI**.

Shadow AI is a PHI risk, not an IT risk

Discovery teams described **not knowing what their clinicians were using.** The first patient name in a consumer LLM is the breach.

Agentic AI makes this worse

Autonomous decisions in prior auth and care management **cannot be governed by point-in-time approval.**

FINDING 04

Six barriers. Written after sitting in on your last governance meeting.

Name the barriers now, before they're raised as objections. Every healthcare organization we work has faced some combination of these factors, almost always more than one.

01 No dedicated owner

AI governance in healthcare is almost never anyone's primary job. It's handed to whoever has relevant expertise: the CISO, the compliance manager, the AI director, the program manager who raised their hand. With no designated owner and no shared platform, there's no accountability and no continuity when that person's role changes.

02 No tooling, or the wrong tooling

88% of organizations don't use a dedicated governance platform. In healthcare, this shows up as governance split across clinical informatics (clinical AI), the CISO's office (security and vendor risk), legal (contracts and HIPAA), and compliance (policy documentation). No single source of truth. Tools like OneTrust, originally built for privacy management, are being repurposed for AI governance in ways that create more documentation burden than they relieve.

03 Fragmented organizational ownership

Healthcare AI governance decisions involve too many stakeholders with no shared visibility: the AI/data team that builds and deploys, the CISO who owns security and vendor risk, legal who owns BAAs, compliance who owns regulatory obligations, and clinical leadership who owns patient safety. Without a shared platform, AI governance becomes a **coordination problem** more than a technical one.

04 Risk tiering doesn't exist

Without a formal risk framework, every use case gets treated the same whether it's a low-risk internal chatbot or a high-risk clinical decision support system influencing patient treatment. This is the direct cause of pilot purgatory. It's also a compliance gap: the EU AI Act, ISO 42001, and Joint Commission all require risk-differentiated treatment of AI systems.

05 AI governance stops at deployment

Pre-deployment approval is the starting line, not the finish line. AI systems drift. Regulatory requirements evolve. Vendor products update without notice. Most healthcare governance programs have no mechanism for continuous monitoring: no alerting when a model's performance degrades, no process for re-review when a vendor changes their data practices, no dashboard showing post-deployment status across the portfolio.

06 The build vs. buy trap

Some organizations try to build their own governance infrastructure like internal registries, custom workflow tools, homegrown risk frameworks. The main problem with this approach for healthcare organizations is that the regulatory landscape (CMS 0057-F, Joint Commission, ISO 42001) evolves faster than internal builds can track. The organizations that tried to build are now shopping for platforms.

FINDING 05

Where the difficulty compounds — the most challenging aspect of AI governance today

% of leaders selecting this as their #1 hardest challenge

41%

3rd-party AI vendor risk
The most acute and least-solved pain point in healthcare.

26%

Centralized visibility across all AI initiatives, the "Wild West" problem.

18%

Manual workflow burden is the operational tax of SharePoint governance.

15%

Regulatory complexity with tracking changes across HIPAA, Joint Commission, ISO, EU AI Act.

FINDING 06

What leading healthcare AI governance programs do differently.

Not aspirational. Operational. The healthcare organizations closing the gap share three concrete characteristics.

01 · INVENTORY

Centralized inventory with clear ownership mapped to every system.

Not a spreadsheet someone is hopefully maintaining. A living, continuously updated registry that includes third-party vendor tools and embedded AI features with a designated owner and risk classification for each entry.

02 · WORKFLOW

Automated, risk-tiered workflows.

Low-risk use cases move through a streamlined approval lane. High-risk clinical AI gets the full review cycle with documented evidence collection at each stage. **The review process is a calibrated, auditable workflow, not a bottleneck.**

03 · LIFECYCLE

Post-deployment monitoring and audit-ready documentation.

Model performance is tracked. Vendor relationships are monitored. Regulatory changes trigger re-review. Documentation, from initial risk assessment through ongoing records, is stored centrally and can be produced on demand.

WHAT THIS MAKES POSSIBLE

Faster AI deployment
Governance questions are answered upfront, not raised as blockers mid-process.

Cleaner audits
Evidence is organized and accessible, not reconstructed under time pressure.

Credible board reporting
AI Leaders can show the governance dashboard, not just describe the governance policy.

Scales with adoption
Twice as many AI systems doesn't mean twice the governance hours.

• Where to start

Three diagnostic questions to take back to your team.

If you answer with "no," you have a governance gap and likely a compliance gap too.

01 **Inventory**

Can you produce a complete list of every AI system in production, including all vendor-embedded tools and AI features in existing platforms, within 24 hours?

02 **Evidence**

If the Joint Commission, your ISO auditor, or your board asked for governance documentation on your **three highest-risk AI systems** today, could you produce it without a fire drill?

03 **Scale**

Is your current governance process — the review workflows, the documentation system, the monitoring approach — designed to handle **twice as many AI systems** as you have today?

NEXT STEP

See how Credo AI closes these gaps for healthcare organizations.

Centralized inventory. Risk-tiered workflows. Continuous monitoring. Audit-ready evidence for clinical AI, vendor AI, and everything in between.

Book a 30-minute conversation →

About Credo AI

Credo AI is the enterprise AI governance platform built to help organizations scale AI safely delivering centralized AI visibility, automated risk management, and compliance-ready reporting across every AI system.

12	30+	F2000
Forrester perfect scores	Global partners	Customers served