Kiteworks

CAPABILITY BRIEF | HEALTHCARE

Securing Healthcare Data Exchange in the AI Era

Unifying Data Governance, AI Control, and Compliance Across Every Channel a Healthcare Organization Uses to Exchange Sensitive Patient Data

Executive Summary

Healthcare operates under one of the tightest regulatory stacks of any sector, has carried the highest per-incident breach cost of any industry for 13 consecutive years, and has moved AI into production faster than its governance can keep up. Regulators are now applying every existing framework -- HIPAA, HITECH, 42 CFR Part 2, the FTC Health Breach Notification Rule, FDA 21 CFR Part 11, GDPR, and state health privacy laws -- to AI agent activity touching protected health information, without waiting for new rules.

The exposure compounds quickly. Healthcare carries the second-largest governance-to-automation gap of any sector, with nearly a third of organizations still relying on manual or periodic compliance processes[1] -- exactly the conditions in which AI deployments outpace the controls meant to govern them. Ambient scribes, prior-authorization agents, and clinical decision support tools reach into PHI through channels that were never designed to provide an attribution trail an OCR investigator could read.

Kiteworks closes the exposure at the data layer: one platform unifying email, file sharing, MFT, SFTP, data forms, APIs, and AI workflows under a single policy engine, audit log, and security architecture.

The Challenge

AI is in production across clinical documentation, ambient scribing, prior authorization, radiology triage, denials management, and patient engagement. The data layer those workflows consume is the layer most healthcare organizations have not extended their governance to.

Most healthcare organizations operate 5 to 10 separate tools for sensitive data exchange -- each with its own policies, audit logs, and gaps. When AI agents reach into all of those channels, fragmentation that was already a compliance liability becomes an AI governance crisis. When an OCR investigator asks who authorized each AI interaction with regulated PHI, the answer becomes a multi-week investigation across fragmented logs and shared service accounts.

The risk is not theoretical. Half of healthcare organizations cite third-party AI handling as a top concern,[1] yet their visibility into partner AI activity remains low -- so even the controls a health system has built end at its own perimeter. Inside that perimeter, 64% of healthcare organizations lack AI anomaly detection and 77% have not tested

At a Glance

- **Healthcare carries the highest per-incident breach cost of any industry -- $7.42 million -- for 14 consecutive years[2]**
- **81% of physicians now use AI in practice, more than double the 2023 rate of 38%[3]**
- **Only 34% of organizations have complete knowledge of where their data is stored[4]**
- **97% of AI-related breaches involved organizations lacking AI access controls; average U.S. breach cost exceeds $10 million[5]**
- **725 large healthcare data breaches exposing more than 133 million records were reported to HHS OCR in 2023[6]**

recovery time or recovery point objectives (RTO/RPO).[7] The result is an environment where an AI-enabled breach can run undetected for weeks, surface only when it triggers a notification obligation, and leave the organization without the evidence package OCR, the FDA, or a class-action plaintiff will demand.

The Kiteworks Solution

Kiteworks is the secure data exchange for healthcare. One platform. One policy engine. One audit log. Built on a hardened virtual appliance with FIPS 140-3 validated cryptography, single-tenant isolation, and tamper-evident audit streamed in real time to the organization's SIEM.

Control

Policy-enforced access and complete attribution across email, file sharing, MFT, SFTP, data forms, APIs, and AI -- one auditor-ready record of every interaction with PHI, human or agent. Attribute-based access control enforces HIPAA minimum necessary at the operation level, so an agent or user authorized to read a folder is not automatically authorized to download, export, or transmit its contents.

AI Governance

Through Kiteworks Compliant AI, including Secure MCP Server, AI agents are cryptographically authenticated, bound to the human authorizer, and governed by attribute-based access on every request. Independent of model, vendor, or model-level guardrails. When the model is updated, replaced, or compromised, the data-layer controls still apply -- meaning compliance does not depend on the integrity of any individual model or AI vendor.

Compliance

Pre-mapped to HIPAA, HITECH, 42 CFR Part 2, the FTC Health Breach Notification Rule, FDA 21 CFR Part 11, ICH/GCP, GDPR, the EU AI Act, state health privacy laws (Washington MHMDA, California CMIA, and others), PCI DSS 4.0, and ISO 27001. Evidence assembles in hours, not weeks. Pre-built dashboards present audit data in the format each assessor expects -- HIPAA Security Rule safeguards, FDA 21 CFR Part 11 audit trails, GDPR Article 32 technical measures -- so the work shifts from collecting evidence to reviewing it.

Anticipated Outcomes

- **Unified governance.** Replace 5 to 10 fragmented tools with one control plane.
- **AI without compounding regulatory risk.** Authenticated identity, policy-enforced access, FIPS 140-3 encryption, and full audit applied to every AI workflow.
- **Audit trails OCR investigators can read.** Real-time SIEM streaming with full attribution.
- **Evidence in hours, not weeks.** On-demand exports ready for OCR investigations, FDA inspections, state attorney general inquiries, and payer audits.
- **Sovereignty for cross-border operations.** In-jurisdiction key custody, geofencing, and data residency for global clinical research.
- **Defensible clinical research workflows.** ICH/GCP-aligned Trial Master File chain of custody, FDA 21 CFR Part 11 electronic-records integrity, and tamper-evident logs that satisfy sponsors, CROs, and inspectors.

Sources

[1] Kiteworks, Data Security and Compliance Risk: 2026 Forecast Report, December 2025.
[2] IBM Security and Ponemon Institute, Cost of a Data Breach Report, 2025.
[3] AMA, 2026 Physician Survey, 2026.
[4] Thales, 2026 Thales Data Threat Report, 2026.
[5] IBM Security and Ponemon Institute, Cost of a Data Breach Report 2025: The AI Oversight Gap, 2025.
[6] HHS Office for Civil Rights, Breach Portal data, AI Security Statistics 2026 Research Report, March 2026.
[7] Kiteworks, Data Security and Compliance Risk: 2026 Forecast Report, December 2025.