nexustek

HEALTHCARE · HIPAA · 2026

IT THAT KEEPS CARE MOVING

The mid-market healthcare provider's guide to HIPAA-aligned infrastructure, cybersecurity, and AI readiness — without building an enterprise IT team to maintain it.

THE LANDSCAPE

Healthcare IT is carrying more pressure than ever.

Rising breach costs. Tightening compliance. A staffing gap that hiring can't close. Legacy infrastructure blocking modernisation.

57.5%

Of all healthcare breaches hit providers directly

THE HIPAA JOURNAL, FEB 2026

$7.42M

Average cost of a healthcare data breach in 2025

IBM COST OF A DATA BREACH REPORT, 2025

279 days

Average time to detect and contain a healthcare breach

IBM, 2025

31M+

Patient records exposed in H1 2025 alone

THE HIPAA GUIDE, JULY 2025

Healthcare has been the most expensive sector for data breaches for **14 consecutive years**. The average breach took 279 days to detect — nearly **five times** HIPAA's 60-day notification window.

IBM COST OF A DATA BREACH REPORT, 2025

73% of IT systems across the healthcare sector are legacy infrastructure — built before modern security standards, cloud architecture, and the current threat environment existed.

PROFOUND LOGIC, SEPT 2025

> Mid-market healthcare providers carry enterprise-level compliance obligations without enterprise IT staffing. The gap between what's required and what's sustainable internally is the problem NexusTek is built to close.

Six Core Challenges

These challenges don't exist in isolation. **They compound**. Legacy infrastructure expands the attack surface. Staffing gaps leave monitoring uncovered. Compliance obligations tighten on top of everything else.

01

Cyber resilience

Healthcare is the most breached sector. 57.5% of breaches hit providers directly. Most mid-market practices have no 24/7 monitoring. Average breach cost: $7.42M. Average detection time: 279 days.

CYBERSECURITY

02

Compliance and auditability

OCR's proposed HIPAA Security Rule updates make encryption and MFA mandatory — no more "addressable" deferral. Annual point-in-time audits no longer satisfy what regulators expect. OCR penalties run from $3,500 to $6.8M per case.

CYBER + CLOUD

03

IT staffing and skills gap

61% of healthcare IT professionals say staffing shortages are directly impacting their work. One or two generalists can't continuously cover helpdesk, security, patching, and compliance simultaneously.

IT OPERATIONS

04

Legacy system modernisation

73% of healthcare IT systems are legacy infrastructure. EHRs, PACS, and departmental applications predate modern security standards and can't be patched safely without disrupting live clinical workflows.

CLOUD

05

Unpredictable IT costs

Emergency support, unplanned hardware replacement, and breach response costs don't appear in the annual budget. Variable IT spend competes directly with clinical and operational priorities.

CLOUD + IT OPS

06

AI readiness and governance

57% of healthcare organisations say reducing administrative burdens through AI is their biggest opportunity. Most can't deploy AI safely against clinical data — PHI governance risk stops pilots before they scale.

DATA + AI

Regulatory Context

OCR's proposed HIPAA Security Rule updates are moving the expectation from periodic compliance to continuous, demonstrable control. Encryption and MFA are no longer "addressable" — they are mandatory. The proposed updates also tighten audit logging requirements and raise the bar for documented incident response that can be produced on demand.

NEXUSTEK'S ROLE

Implement and manage the technical and operational controls these frameworks require — MFA, encrypted infrastructure, continuous monitoring, incident response procedures, and documented audit trails. NexusTek executes the controls. Demonstrating compliance is the organisation's responsibility.

HIPAA Security Rule

ALL COVERED ENTITIES + BUSINESS ASSOCIATES

- Mandatory encryption at rest and in transit — "addressable" status removed under proposed updates
- Mandatory MFA for all access to systems containing ePHI
- Full audit logging with tamper-proof trail across all ePHI systems
- Documented risk analysis completed annually, not as a one-time project

HIPAA Breach Notification Rule

60-DAY NOTIFICATION WINDOW VS. 279-DAY DETECTION AVERAGE

- Covered entities must notify affected individuals within 60 days of discovering a breach
- OCR must be notified of breaches affecting 500+ individuals within 60 days
- Healthcare breaches averaged 279 days to detect in 2025 — 4.6x the notification window
- 24/7 MDR and SOC monitoring is the structural answer to the detection gap

NIST CSF 2.0 + HPH CPGs

CYBERSECURITY FRAMEWORK ALIGNMENT

- HHS Healthcare and Public Health Cybersecurity Performance Goals define Essential and Enhanced control tiers
- NIST CSF 2.0 Govern function requires cross-organisational ownership of cybersecurity risk
- Cyber insurers increasingly reference HPH CPGs and NIST CSF as the baseline for controls questionnaires
- NexusTek Security Assessment maps posture against all three frameworks simultaneously

NIST AI Risk Management Framework

AI GOVERNANCE FOR HEALTHCARE DEPLOYMENTS

- NIST AI RMF Govern function requires documented AI risk ownership and policies before deployment
- PHI used as AI model input creates HIPAA exposure if the environment is not controlled and auditable
- NexusTek Secure AI Platform provides the governed infrastructure layer NIST AI RMF requires
- AI Readiness Assessment maps the path from experimentation to compliant production deployment

IN PRACTICE

Two real engagements. Two kinds of problems NexusTek solves.

A mental health nonprofit with a stretched IT team. A health equity foundation with a research data bottleneck. Both needed a partner that understood what healthcare organisations actually require.

MENTAL HEALTH | NONPROFIT
300+ EMPLOYEES | FULLY MANAGED IT

A 300-person mental health nonprofit regains consistent clinical system access.

A growing organisation with an internal IT team stretched beyond capacity. Their existing MSP wasn't delivering. Infrastructure demands had outpaced what internal resource could manage. Clinical staff were losing reliable access to patient systems.

THE SITUATION

- 300+ clinical and administrative staff dependent on consistent system access
- Existing MSP relationship not delivering adequate service level
- Internal IT team handling helpdesk, specialist projects, and infrastructure simultaneously
- No proactive monitoring or patch governance in place

WHAT NEXUSTEK DELIVERED

- Fully Managed IT Services — NexusTek took over daily IT network operations
- Proactive monitoring, hardware updates, patch management across all systems
- Firewall management and cybersecurity baseline implemented
- Dedicated Service Delivery Manager appointed from day one
- Weekly cadence calls, status updates, issue resolution, and forward planning

Clinical staff. Consistent access. Zero distraction.

WHAT CHANGED

Clinical and administrative staff regained reliable, consistent access to applications and patient data. The internal IT team was refocused on strategic projects rather than reactive infrastructure management.

The dedicated SDM model — weekly calls, documented next steps, proactive issue tracking — is what distinguishes a managed IT partner that works from one that doesn't.

> We always know what we're doing, what the next steps are, and when those are due. They've got a very good process to accomplish what we need.

IT Director, 300+ employee nonprofit mental health organisation. This quote describes the weekly cadence call structure and dedicated SDM model specifically — the experience of working with NexusTek, not just the outcome.

HEALTH EQUITY | NONPROFIT
AI + PRIVATE CLOUD | RESEARCH AUTOMATION

Episcopal Health Foundation cuts research time by up to 5x with a custom AI tool.

A Texas-based health equity nonprofit was drowning in research data with no scalable way to extract insight. Manual analysis took 5–10 hours per research area. Governance and compliance requirements made generic AI tools off-limits.

THE SITUATION

- Research data volumes growing faster than the team could manually process
- 5–10 hours per research area for manual analysis — hundreds of hours across programs
- No internal AI expertise; strict data governance requirements throughout
- Tight programmatic deadlines with no capacity to build internally

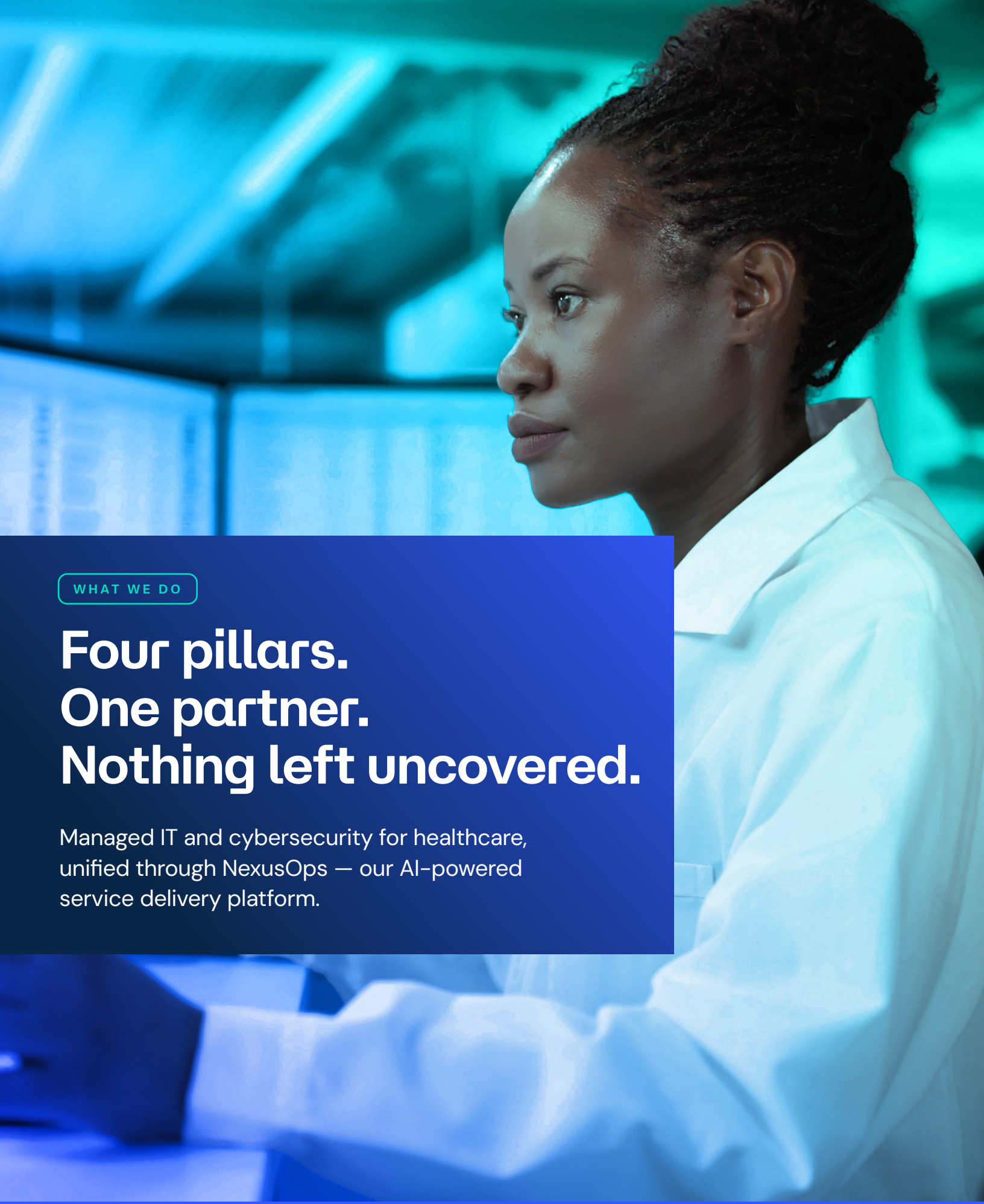
WHAT NEXUSTEK DELIVERED

- Custom AI tool built using NLP to analyse research libraries and surface actionable intelligence
- Migration to NexusTek Private Cloud — hybrid architecture for scalability and availability
- Encrypted architecture and role-based access controls implemented throughout
- Staff training on responsible AI use with governance controls from day one
- **Research time cut by up to 5x. Governance built in.**

WHY THIS MATTERS FOR HEALTHCARE AI

The EHF engagement demonstrates the only safe path to AI adoption in a data-sensitive environment: governed infrastructure first, deployment second. The Secure AI Platform and private cloud provide the controlled boundary that keeps sensitive data within a compliant environment.

For healthcare organisations with research, billing automation, or administrative AI ambitions, the question is not whether AI is possible — it's whether the governance infrastructure exists to deploy it safely.



WHAT WE DO

Four pillars. One partner. Nothing left uncovered.

Managed IT and cybersecurity for healthcare, unified through NexusOps — our AI-powered service delivery platform.

Cloud

Private, hybrid and HIPAA-aligned

Data + AI

Governed AI within compliant boundaries

IT Operations

Fully Managed, Co-Managed, vCIO

Cybersecurity

MDR, 24/7 SOC, vCISO

01

CLINICAL SYSTEMS THAT STAY AVAILABLE

Cloud

HIPAA-aligned Tier 4/5 Private Cloud with encryption at rest and in transit, granular RBAC, and full audit logging. 99.9% uptime SLA. Fixed-cost billing eliminates variable egress charges. Hybrid architecture keeps legacy clinical systems available during phased migration. 100% cloud migration success rate.

> 100% cloud migration success rate · 99.9% uptime SLA on NexusTek Private Cloud · Tier 4/5 data centre hosting

02

GOVERNED AI ADOPTION

Data + AI

NexusTek Secure AI Platform provides governed access to leading generative AI models within a controlled, HIPAA-aligned environment — ePHI never reaches an unmanaged third-party system. AI Readiness Assessment maps the specific use cases where AI delivers measurable operational value and identifies the infrastructure gaps that must close before production deployment. GPU-enabled Private Cloud for inferencing workloads.

> 57% of healthcare organisations cite admin automation as their biggest AI opportunity — the EHF case study demonstrates what governed AI deployment looks like in practice

03

THE IT TEAM YOUR ORGANIZATION NEEDS

IT Operations

Fully Managed IT or Co-Managed IT provides the full capability layer as an external function — proactive monitoring, patch management, service desk, and infrastructure management through NexusOps with NexusIQ. 97% triage accuracy routes every ticket to the right engineer without human sorting. Root cause identification 90% faster. vCIO for IT strategy aligned to clinical and operational budgets. vCISO for executive-level security programme leadership on demand.

> 97% triage accuracy · 90% faster root cause identification · 78% faster automated status updates via NexusOps with NexusIQ

04

BUILT FOR HEALTHCARE'S THREAT ENVIRONMENT

Cybersecurity

MDR and 24/7 SOC closing the 279-day detection gap that defines the healthcare breach problem. AI Email Security stops phishing before it reaches clinical inboxes — the primary breach vector for mid-market providers. EDR across clinical workstations. MFA and IAM as mandatory controls under OCR's proposed HIPAA Security Rule updates. Security Assessments mapping posture against HIPAA Security Rule, NIST CSF 2.0, and HPH CPGs. vCISO on demand for organisations that need executive security leadership without a full-time hire.

> Healthcare: most expensive sector for data breaches for 14 consecutive years · NexusTek Security Assessment addresses HIPAA, NIST CSF 2.0, and HPH CPGs simultaneously

WHO WE SERVE

Five sub-segments. Different buyers, different entry points, different conversations that open the door.

Physician groups + multi-specialty practices

Practice Administrators · COOs · Office Managers

Challenge: No dedicated internal IT function. Technology decisions land on the Practice Administrator alongside clinical ops, billing, HR, and compliance. EHR downtime stops patient care immediately.

NexusTek: Fully Managed IT and cybersecurity as a single fixed-cost partner. Security Assessment as the entry point.

> *"If your EHR went down this afternoon, who gets the call, what happens to patients already in the building, and how long before you're back up?"*

FULLY MANAGED IT | SECURITY ASSESSMENT | HIPAA

Community hospitals + regional health systems

IT Directors · VP IT · CIO · COO or CFO

Challenge: Internal IT team exists but lacks security depth. Mix of legacy clinical systems and modern cloud across multiple sites. Compliance obligations are formal but continuous governance is absent.

NexusTek: Co-Managed IT covering the layers the internal team cannot sustain continuously. 24/7 SOC, patch governance, vCISO.

> *"Your internal IT team keeps the lights on. What happens to your security posture and compliance position when they're dealing with an active incident at the same time?"*

CO-MANAGED IT | MDR + SOC | VCISO

Outpatient + ambulatory care centers

Practice Administrators · Operations Directors · COOs

Challenge: Tight scheduling margins — every appointment slot is revenue. System downtime stops the care delivery workflow entirely. Multi-site environments accumulated through growth, not design.

NexusTek: Managed IT and cybersecurity that keeps clinical systems available during operating hours across every location.

> *"You run a full schedule every day. What does one hour of system downtime cost you in cancelled procedures, rescheduled patients, and staff time?"*

FULLY MANAGED IT | SECURITY ASSESSMENT | MULTI-SITE

Diagnostic labs + imaging centers

Operations Directors · IT Managers · COOs

Challenge: PACS, imaging workstations, and lab systems generating high data volumes with specific availability requirements. Over 83% of internet-connected medical imaging devices still run outdated software.

NexusTek: Security Assessment plus DRaaS with tested recovery RTOs built around the availability requirements imaging workflows demand.

> *"If ransomware encrypted your imaging system tonight, how long would it take to restore read access for your radiologists?"*

SECURITY ASSESSMENT | DRAAS | LEGACY SYSTEMS

Telehealth + remote care providers

CTOs · IT Directors · COOs · VP of Operations

Challenge: No physical perimeter. Attack surface is the platform itself. Phishing targeting clinician credentials is the primary breach vector. Platform availability is the product — downtime is a direct service failure.

NexusTek: AI Email Security, Secure Remote Access, and 24/7 SOC monitoring built for digital-first care delivery environments.

> *"Your clinicians and patients connect from devices and networks you don't control. What visibility do you have into whether those sessions are secure?"*

AI EMAIL SECURITY | SECURE REMOTE ACCESS | MDR

WHY NEXUSTEK

Healthcare IT outcomes. Without building the capability internally.

The managed IT and cybersecurity partner for operators that need to run reliably and securely.

WHY NEXUSTEK

Full compliance stack under one partner

Security Assessments, HIPAA-aligned Private Cloud, MDR, DRaaS, and vCISO services. One contract. One escalation path. One audit trail that holds up to an OCR review.

100% cloud migration success rate

Every cloud migration NexusTek has completed ran without clinical disruption. Cloud Readiness Assessment sequences workloads by clinical risk so the systems staff depend on move last, not first.

Tier 4/5 infrastructure — not public cloud

NexusTek Private Cloud is hosted in Tier 4 and Tier 5 data centres with fixed-cost billing and granular access controls designed for ePHI environments from the ground up.

A governed path to AI adoption

Secure AI Platform keeps ePHI inside a HIPAA-aligned boundary. AI Readiness Assessment maps the path from pilot to production. The EHF case study is the proof: research time cut by up to 5x.

NexusOps offsets the staffing gap

97% triage accuracy. Root cause 90% faster. 78% faster automated status updates. For organisations that can't hire their way out of the staffing problem, this is a structural answer.

Executive security leadership on demand

vCISO delivers CISO-level function — formal security programme, policy framework, OCR relationship management, and ongoing executive oversight — without the full-time hire cost.

99.9%	100%	98%	1,200+	~30 yrs
Uptime SLA, Private Cloud	Cloud migration success	Client satisfaction rating	Active clients	IT services experience

Start with a Security Assessment.

Map your current environment against HIPAA Security Rule requirements, NIST CSF 2.0, and HPH CPGs. Identify the gaps creating the most compliance and operational risk. Get a prioritised remediation roadmap — useful regardless of whether you engage NexusTek further.

SCHEDULE YOUR ASSESSMENT

Learn more at nexustek.com

(877) 470-0401 • info@nexustek.com

Protect Your Contracts. Achieve CMMC 2.0.
nexustek.com · (877) 470-0401 · info@nexustek.com

nexustek