AI in Healthcare Cybersecurity:
Risks, Compliance, and Practice

Summer CPE Symposium, Session #4

June 24, 2026

Presented by:

John K. Cross, Consulting Principal

Introductions

John K Cross

Consulting Principal

Information Technology Consulting

jcross@pyapc.com

Learning Objectives

1. Describe the current healthcare cybersecurity threat landscape, including key breach statistics, threat actors, and attack vectors targeting healthcare organizations. Classify AI use in Cybersecurity vs. AI tools use.
2. Identify how artificial intelligence is being weaponized by threat actors through deepfakes, polymorphic malware, and AI-enhanced social engineering campaigns.
3. Explain how AI-driven defensive technologies (SOC automation, behavioral analytics, threat intelligence) are transforming cybersecurity operations in healthcare.
4. Apply relevant governance and risk frameworks including NIST CSF, NIST AI RMF, and the pending HIPAA Security Rule updates to evaluate and manage AI-related cyber risks.
5. Recommend actionable risk-mitigation steps and governance strategies that organizations can adopt to assess and strengthen AI cybersecurity readiness.

Agenda

1. The Threat Landscape
   - ✓ Healthcare by the numbers, case studies, patient safety impact
2. AI as Intrusion
   - ✓ AI-powered phishing, deepfakes, polymorphic malware, DaaS
3. AI as Intelligence
   - ✓ AI-powered SOC, behavioral analytics, Zero Trust, AI-orchestrated defense
4. Governance and Frameworks
   - ✓ NIST CSF + AI RMF, HIPAA Security Rule, HSCC guidance, legislation
5. Putting It into Practice
   - ✓ A framework for assessing AI cybersecurity readiness, key questions, and practical next steps.

The Threat Landscape

Healthcare Cybersecurity Facts

$7.42M

IBM Cost of Data Report 2025
(highest across all industries, last 14 years)

276M+

Health records affected by healthcare breaches in 2024 alone

279 Days

Average time to identify and contain a HC breach
(241 days globally across all industries)

93%

Of healthcare orgs experienced ≥1 cyberattack (past 12 months)

1,710

Healthcare incidents w/1,542 confirmed disclosures

1% to 16%

YoY increase in espionage as motive (nation-state actors)

Sources: HIPAA Journal (2026); Proofpoint-Ponemon Institute (2025); Seceon Whitepaper (2025)

How Are the Security Risks Generated by AI Unique, Different, and New?

Securing the IT infrastructure

Information technology security (IT security) is a broad, multifaceted measure of protection for a computer **network** and its **data** from any breach, leak, publication of private information, or attack.

VS.

Securing AI

AI security involves defending AI **models**, **algorithms**, and **data** from manipulation, misuse, or unauthorized access to ensure systems perform as intended.

Types of AI Tools

Simplified AI Classification for Risk Assessment

AI/ML Analytics Platform

Traditional ML systems that analyze structured data to identify patterns, predict outcomes, and support clinical decisions.

Examples:

- Predictive models for patient risk scores
- Readmission forecasts
- Disease progression analytics

Generative AI SaaS

Cloud-based AI services that create new content (text, images, code) from prompts or inputs.

Examples:

- Clinical documentation assistant
- Patient communication chatbots
- Medical imaging interpretation tools
- Ambient scribe solutions

AI Data Processing

Background AI systems that organize, transform, or enrich data without direct user interaction.

Examples:

- Automated medical coding
- PHI de-identification tools, claims adjudication, or real-time data extraction from EHRs

The Hidden Complexity

Traditional vs. AI Technology Stacks

- AI systems involve asynchronous co-evolving processes, multiple artifacts (code + data + models), continuous monitoring, and specialized tooling.
- They are inherently more complex and difficult to audit than traditional software.

Traditional Software Tech Stack	AI/ML Tech Stack	
Total Components: 3-5 core layers	**Total Components:** 5-7+ interconnected layers	
• **Application Layer**: User interface & business logic • **Data Layer**: Structured databases (SQL) • **Infrastructure**: Servers, networking, storage	• **Governance Layer**: Security, ethics, compliance frameworks • **Application Layer**: Prompts, evaluation, AI interfaces • **Model and Orchestration**: LLMs, training, MLOps pipelines	• **Data Engineering**: Vector embeddings, feature stores, versioning • **Infrastructure**: GPUs/TPUs, elastic compute, specialized hardware
Artifacts: Source code is primary asset	**Artifacts:** Data + models (not code) are primary assets	
Governance: Code review, version control	**Governance:** Model registries, drift monitoring, continuous retraining	

Cyberattacks Are Clinical Events, Not Just IT Events

The 2025 Proofpoint-Ponemon study surveyed 677 IT/security professionals across U.S. healthcare

Ransomware-delayed care contributed to an estimated 42–67 Medicare patient deaths between 2016–2021.

72%
Reported disruption to patient care delivery

54%
Reported increased medical procedure complications

29%
Reported increased mortality rates

> "Patient safety is inseparable from cyber safety."

Ryan Witt, VP Industry Solutions, Proofpoint

Sources: Proofpoint-Ponemon Institute (2025); DeepStrike Healthcare Breach Analysis(2025)

Case Study: Change Healthcare Ransomware Attack

The largest healthcare data breach in U.S. history, **triggered by one missing MFA control.**

FEB 12, 2024 — ALPHV/BlackCat gains access via stolen credentials; system lacked MFA

FEB 12–21, 2024 — Attackers move laterally for 9 days, exfiltrating data

FEB 21, 2024 — Ransomware deployed, 100+ systems shut down; nationwide claims halted

APRIL 2024 — UnitedHealth pays $22M ransom; RansomHub demands second ransom

2024–2025 — 192.7 million individuals affected — **~more than half of all Americans**

2025–2026 — UHG under DOJ criminal investigation; OCR HIPAA compliance investigation; 49 lawsuits

$2B

Estimated total cost (FY2024)

40%

Of all U.S. claims processed through Change Healthcare

192.7M

Individuals affected — largest breach ever

Case Study: Ascension Health Ransomware Attack

- **What happened…**
  - May 8, 2024: IT team detects unusual network activity
  - Employee accidentally downloaded a malicious file
  - Black Basta* ransomware group encrypted servers
  - EHR systems offline across 140 hospitals in 19 states
  - Doctors/nurses resorted to pen and paper
  - 6 weeks to fully restore electronic health records
- **Impact and lessons:**
  - 5.6 million patient records compromised
  - EMS diversions — delayed emergency care
  - Month-long disruptions: labs, prescriptions, procedures
  - $1.1 billion net loss for fiscal year (June 2024)
  - Only 7 of 25,000 servers accessed — but double extortion

Insight:
A single employee click + inadequate endpoint controls = system-wide catastrophe

***Black Basta, the ransomware group responsible, was disrupted by law enforcement in early 2025**

AI as Intrusion

How AI Is Weaponized Against Healthcare

AI-Enhanced Phishing

GenAI crafts context-aware phishing at scale

442% surge in phishing (H1→H2 2024)

Bypasses signature-based filters

Deepfakes & Voice Cloning

Realistic exec/clinician impersonation

$25M stolen via deepfake CFO call (Arup)

51% of businesses targeted; 43% fell victim

Polymorphic AI Malware

AI rewrites code on each execution

560,000 new variants detected daily

BlackMamba PoC: GPT generates payloads at runtime

Nation States (Volt Typhoon) have entered the game

Deepfake-as-a-Service (DaaS)

DaaS exploded in 2025 — low barriers

Gen AI fraud: $65B+ projected losses by 2028

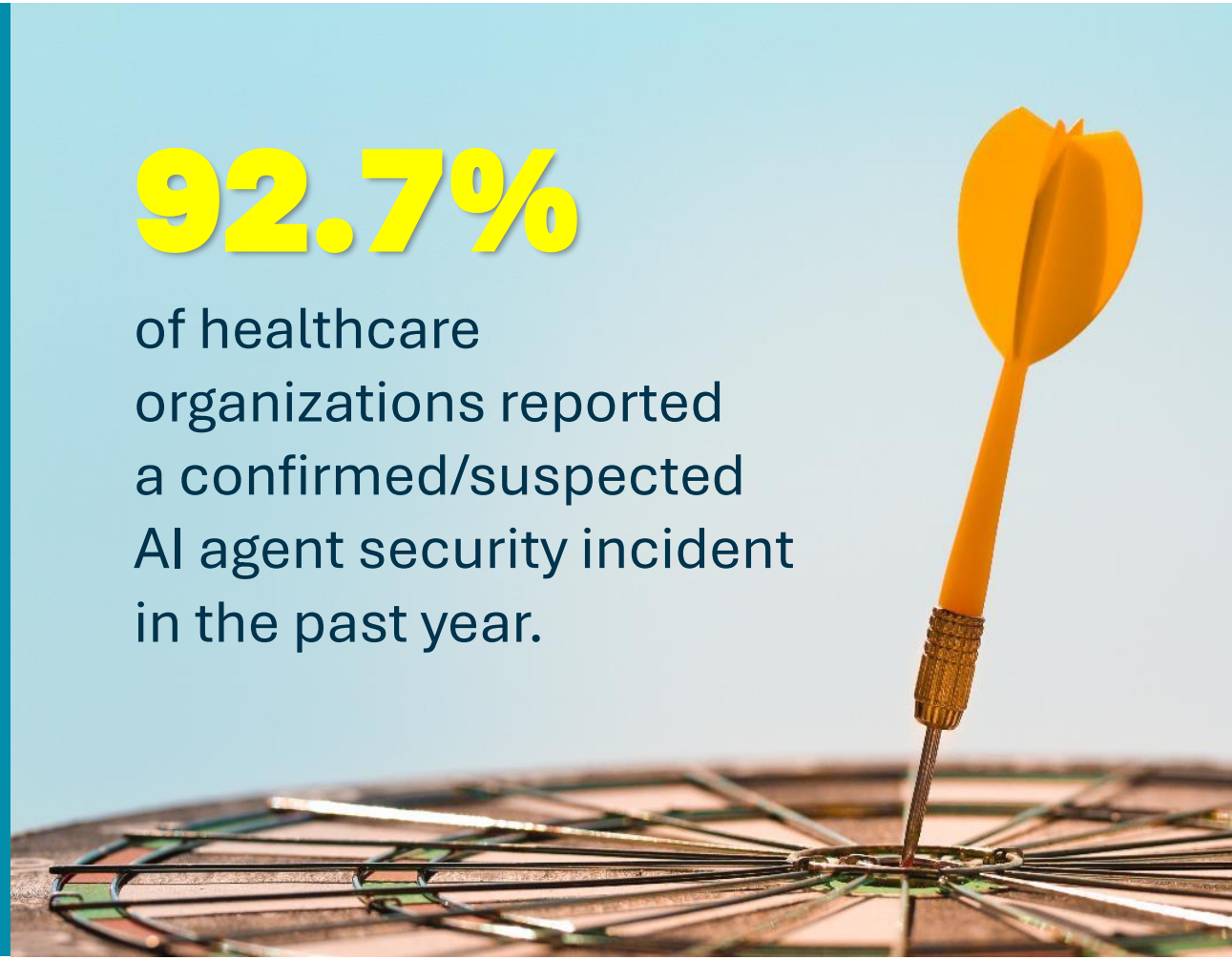
Targets healthcare, finance, government

Sources: CrowdStrike (2025), Health-ISAC (2026), Cyble (2025), Jericho Security (2025)

How AI Is Weaponized Against Healthcare (cont.)

- **Agentic AI Exploitation**
  - AI agents with EHR/device access are now primary ransomware targets
  - “Lethal trifecta”: access to private data + ability to exfiltrate + exposure to untrusted content
  - Prompt injection allows hijacking of autonomous clinical agents

Sources: CrowdStrike (2025), Health-ISAC (2026), Cyble (2025), Jericho Security (2025), Gravitee's 2026 "State of AI Agent Security" report



Deepfakes: The Healthcare-Specific Threat

- Attack scenarios
  - **Executive impersonation:** Fake CEO/CFO communications directing wire transfers or PHI access changes
  - **Clinical impersonation:** Fake physician voice directing medication changes
  - **Telemedicine fraud:** Deepfake patients obtaining controlled substances
  - **Insurance fraud:** Synthetic identities filing false claims
  - **Social engineering:** AI-generated 'urgent' voicemails from leadership
  - **AI Agent Impersonation:** Compromised agentic AI systems simultaneously exfiltrate records while altering medication dosages, deleting allergy warnings, and corrupting lab results

Sources: HealthManagement.org (2026), Cyflare (2025), CardinalOps (2025)

Deepfakes: The Healthcare-Specific Threat (cont.)

- Why healthcare is uniquely vulnerable
  - **Culture of urgency:** "Stat" orders bypass normal verification
  - **Trust hierarchies:** Physicians' verbal orders routinely followed
  - **Value of data:** PHI sells 25-50x more than credit cards on dark web
  - **Distributed workforce:** Telehealth, remote coding, outsourced billing

Questions Worth Asking:

- Does your organization have a deepfake awareness program?
- Are verbal authorization procedures verified through a secondary channel?

Sources: HealthManagement.org (2026), Cyflare (2025), CardinalOps (2025)

AI as Intelligence

AI-Powered Cyber Defense in Healthcare

74%
Of mid-to-large orgs deployed AI-powered threat detection

67%
Shifting to behavior-based detection strategies

88%
Anticipate AI will significantly impact detection within 3 years

	Current AI Defense Capabilities	The Future: AI-Orchestrated SOCs
Automated alert triage	Filters false positives, reduces SOC burnout	Shift from "AI-assisted" to "AI-orchestrated" operations
Real-time detection	Identifies compromised accounts within seconds	Autonomous agents coordinating tools under policy guardrails Humans retain authority for patient-safety-critical systems
Behavioral analytics	Models normal clinical workflow patterns	Detection will model patient care pathways and device norms
Automated compliance	Continuous HIPAA/CMS monitoring and reporting	Autonomous containment

Sources: SANS/Anvilogic Detection Engineering Survey (2025); ACSMI Report (2026); HealthTech Magazine (2025)

The AI Arms Race: Attack vs. Defense

Dimension	AI as Weapon (Intrusion)	AI as Shield (Intelligence)
Phishing	GenAI creates personalized phishing at scale	NLP analysis flags anomalous patterns
Malware	Polymorphic code evades signature detection	Behavioral analysis detects execution patterns
Identity	Deepfake audio/video impersonates users	Anomaly detection flags unusual access
Network	AI-driven recon maps networks faster	Baseline traffic modeling detects lateral movement
Speed	Ransomware encrypts in <4 days	Automated containment within seconds
Scale	DaaS lowers barriers for any actor	AI scales across cloud, on-prem, IoMT
Agentic Systems	AI agents hijacked via prompt injection to exfiltrate PHI and alter clinical data	Agent orchestration platforms with RBAC, audit trails, and continuous red-teaming

The Paradox:
Detection takes 241 days on average vs. ransomware encryption in <4 days.
Unified, AI-driven defense is no longer optional.

Governance and Frameworks

NIST CSF + AI RMF: A Unified Approach

- **NIST Cybersecurity Framework (CSFv2)**
  - **Identify:** Catalog AI tools handling PHI
  - **Protect:** Access controls, encryption, secure configs
  - **Detect:** Monitor for AI-enabled attack patterns
  - **Respond:** Incident response including AI-specific events
  - **Recover:** Coordinate with AI governance post-incident

- **NIST AI Risk Management Framework (AI RMF)**
  - **Govern:** Policies, roles, risk thresholds for AI
  - **Map:** Context, stakeholders, technical & societal impacts
  - **Measure:** Bias testing, safety evaluation, ongoing monitoring
  - **Manage:** Treat, transfer, or accept AI-specific risks

Note:

- *NIST AI RMF GenAI Profile(NIST-AI-600-1, July 2024) now formally part of the RMF*
- *AI RMF Profile for Critical Infrastructure is released as a concept note (April 2026)*

Integration Point:

- **Extend CSF's "Detect and Respond" to cover AI-specific risks (data poisoning, model manipulation, drift); coordinate CSF's "Recover" with AI RMF's "Govern" to refine policies after incidents. *EU AI Act maps to NIST AI RMF.**
- **Healthcare organizations should integrate both NIST frameworks to address traditional cybersecurity and AI-specific risks; HHS bases its AI risk guidance on these frameworks.**

Sources: NIST AI RMF 1.0 (2023); Censinet (2025), HHS AI Strategy (2025)

Regulatory Landscape: What's Changing

Proposed HIPAA Security Rule Update

- Published Jan 6, 2025 by HHS OCR, first major update in 10+ years: Aligns with NIST CSF and HHS CPGs.
- Finalization expected late 2026 / early 2027
- The "required vs. addressable" distinction is being eliminated; ALL implementation specs become required
- Brings AI into scope

HSCC 2026 AI Cybersecurity Guidance

- Full AI Cybersecurity Governance Guide released Jun 2, 2026
- Addresses EHR, diagnostics, and DSS; covers ML, GenAI, and Agentic AI
- Aligns with FDA, NIST AI RMF, CISA

Healthcare Cybersecurity Act of 2025

- Establishes CISA-HHS partnership with dedicated liaison
- Mandates tailored threat intelligence and training for healthcare

Sources: HHS OCR (2025), Alston & Bird (2025), HSCC (2025), White House (2025)

Regulatory Landscape: What's Changing (cont.)

Trump Executive Orders on AI (2025-present)

- EO 14179, "Removing Barriers to American Leadership in Artificial Intelligence" (Jan 25)
- "Advancing Artificial Intelligence Education for American Youth" (Apr 25)
- "Accelerating Federal Permitting of Data Center Infrastructure" (Jul 25)
- "Preventing Woke AI in the Federal Government" (Jul 25)
- "Promoting the Export of the American AI Technology Stack" (Jul 25)
- EO 14355, "Unlocking Cures for Pediatric Cancer with Artificial Intelligence" (Sep 25)
- EO 14365, "Ensuring a National Policy Framework for Artificial Intelligence" (Dec 25)
- EO 14409, "Promoting Advanced Artificial Intelligence Innovation and Security" (Jun 26)

CISA Cyber Incident Reporting (CIRCIA)

- Proposed rulemaking requires healthcare to report cyberattacks within 72 hours and ransomware payments within 24 hours.
- Final rule pending.

Practical Action Step:

- The proposed HIPAA Security Rule will eliminate the “required" vs. "addressable” distinction (MFA, TLS1.2+, encryption in transit, annual pen testing, biannual vulnerability scans, etc.)
- Begin gap assessments against the proposed requirements **NOW**.

Sources: HHS OCR (2025), Alston & Bird (2025), HSCC (2025), White House (2025)

AI-Specific Risks Healthcare Auditors Must Know

- **Data poisoning:** Attackers manipulate training data to corrupt AI outputs
  - Could cause misdiagnoses, incorrect medication recommendations, or biased triage decisions
- **Model drift:** Performance degrades as real-world data diverges from training data
  - Without monitoring, clinical AI tools may silently become less accurate
- **Model manipulation:** Adversarial inputs cause incorrect outputs
  - Example: Altering medical imaging pixels to hide or fabricate tumors in AI-analyzed radiology
- **PHI in training data:** AI models trained on patient data may memorize and leak PHI
  - Evaluate whether AI vendors' training processes adequately protect ePHI
- **Agent/Agentic System Risks:** Multi-agent AI systems interact autonomously with EHR, pharmacy, imaging, and device networks
  - Risks include:
    - ✓ AI-to-AI interaction amplifying errors across systems
    - ✓ Memory accumulation leaking PHI across sessions
    - ✓ Prompt injection hijacking agent chains
    - ✓ Emergent hierarchies where one agent improperly dominates others

Sources: HSCC Cybersecurity Working Group (2025); Ogletree Deakins (2025); NIST AI RMF 1.0; JMIR March 2026

AI-Specific Risks Healthcare Auditors Must Know (cont.)

Emerging Threat: "Harvest Now, Decrypt Later"

Attackers steal encrypted data today, anticipating quantum computing will allow decryption.
This amplifies the long-term risk of every data breach (*See *post-quantum cryptography standards (FIPS 203, 204, 205)*)

Sources: HSCC Cybersecurity Working Group (2025), Ogletree Deakins (2025), NIST AI RMF 1.0

Healthcare AI Security Review Process

Traditional vs. AI-Enabled Environments

AI systems require **ongoing** risk **assessments**, ***not* annual** reviews**.** Healthcare organizations must evaluate what PHI the model processes, whether outputs are human-reviewed, and if training data includes PHI, etc.

Traditional Security Reviews	With AI Systems – All Traditional Security Review Steps, PLUS…
Vendor surveys: HIPAA, SOC2, ISO	AI risk classification (patient safety impact, PHI sensitivity, automation level)
Compliance documentation	Training data governance review
Risk classification (L/M/H)	Adversarial testing (prompt injection, data poisoning)
Annual security assessments	Model transparency assessment
BAAs	Bias and fairness evaluation
Pen testing	BAA with AI-specific clauses (data reuse, prompt storage)
Review timeframe: 2-4 weeks+	Continuous monitoring of model drift
	Review timeframe: 6-12 weeks+/continuous
	AI bill of materials
	Agentic AI review (permissions, audit trail, prompt injection resilience)

Putting It Into Practice

AI Cybersecurity Readiness Framework for Healthcare

1. Governance & Oversight

- Does a formal AI governance policy exist?
- **Does a formal AI governance board/process exist?**
- Is there board-level reporting on AI cyber risks?
- **Are AI deployments inventoried and risk-classified?**
- Are roles/responsibilities defined for AI oversight?

2. Risk Assessment

- Has the org assessed AI-specific risks (poisoning, drift, bias)?
- **Are third-party AI vendors included in risk assessments?**
- **Is there a process for evaluating AI tools before deployment?**
- Are PHI exposures in AI training data evaluated?
- Has the org assess post-quantum cryptography risk?

3. Technical Controls

- Is MFA enforced on all remote access systems?
- Are AI-powered detection/response tools deployed?
- Are behavioral analytics monitoring clinical workflows?
- **Are Zero Trust architectures implemented?**

4. Incident Response & Recovery

- Does the IR plan address AI-specific incidents?
- Are deepfake scenarios included in annual training and tabletop exercises?
- **Is there post-incident AI model revalidation?**
- Are RTOs adequate for patient safety?

Pro Tip:
Map your risk assessment activities to both NIST CSF AND NIST AI RMF functions for comprehensive coverage aligned with HHS expectations.

11 Questions Every Healthcare Leader Should Ask

- **For the CISO / IT Leadership**
  - Is MFA implemented on every remote access point?
  - What AI tools are deployed in security operations, and how are they validated?
  - How do we detect AI-generated phishing and deepfake attacks?
  - What is our mean time to detect (MTTD) and mean time to respond (MTTR)?
  - Are deepfake scenarios included in IR tabletop exercises?

- **For the Board / Governance Committee**
  - Do we have an AI governance policy for both operational AI and AI cyber threats?
  - What is our financial exposure to a Change Healthcare-scale event?
  - What is our gap status against the HIPAA Security Rule final rule, specifically mandatory MFA, mandatory encryption, and mandatory penetration testing?
  - How are third-party AI vendors assessed for security and PHI handling?
  - What is our roadmap for integrating NIST AI RMF into risk management?
  - Do we have a post-quantum cryptography roadmap for long-retention PHI given NIST's finalized PQC standards?

Practical Implementation Procedures: AI Cybersecurity

Focus Area	Procedure	Framework Reference
AI Inventory	Verify completeness of all AI tools deployed (clinical, operational, security)	NIST AI RMF — Map
Vendor Risk	Review AI vendor contracts for PHI safeguards, data retention, model training	HIPAA §164.314
Access Controls	Test MFA implementation across all remote access and privileged accounts	NIST CSF — Protect
Detection Efficacy	Review SOC metrics: false positive rate, MTTD, MTTR; evaluate AI tools	NIST CSF — Detect
Phishing Resilience	Review AI-enhanced phishing simulations; assess deepfake awareness training	NIST AI RMF — Manage
Bias and Drift	Verify clinical AI tools have ongoing performance monitoring and bias testing	NIST AI RMF — Measure
IR Readiness	Review tabletop exercises for AI-specific scenarios (deepfake, data poisoning)	NIST CSF — Respond
Regulatory Gap	Perform gap assessment against HIPAA Security Rule (Pending finalization 2026)	HHS OCR Proposed Rule
Agentic AI Controls	Inventory all AI agents; verify identity scoping, permission gating, and audit trail completeness	NIST AI RMF GenAI Profile
Post-Quantum Readiness	Assess encryption standards in use; identify long-retention PHI at risk from future quantum decryption	NIST FIPS 203/204/205

Types of AI Tools & Recommended SOC 2 TSCs*

	Recommendation		
AI Tool Types	**Recommended TSCs**	**Why?**	**Examples**
AI/ML Analytics Platform	Security + Processing Integrity + Availability	Helps ensure reliable, accurate outputs with expected uptimes.	• **Risk-stratification and population health:** Platforms like Azure Health Insights and IBM Watson Health analyze EHR and claims data to flag high-risk patients, optimize care pathways, and support oncology treatment decisions. • **Quality and operations analytics:** Tools that mine hospital data for readmission risk, ED overuse, or LOS optimization, then surface dashboards for clinicians and administrators.
Generative AI SaaS	Security + Availability + Confidentiality + Privacy	Helps protect proprietary models and user data.	• **Clinical documentation assistants:** Solutions such as Nuance DAX or similar ambient listening tools record clinician–patient encounters, transcribe, summarize, and draft notes directly into the EHR. • **Patient and staff copilots:** Generative chatbots used for medical FAQs, post-discharge follow-up, appointment reminders, and summarizing patient communication, etc.
AI Data Processing	Security + Processing Integrity + Confidentiality	Focuses on accurate, secure data handling.	• **PHI de-identification services:** Vendors that use NLP and deep learning to automatically remove identifiers from clinical notes, images, and other records so data can be used for research while staying HIPAA-compliant. • **Anonymization and Synthetic data processing:** Services that mask identifiers, generalize dates, or generate synthetic patient data sets to allow model training and analytics without exposing real patient identities

*** SOC 2 Trust Services Criteria are the standard categories used to evaluate a vendor's security controls**

Key Takeaways

Innovation

AI defense tools are essential; 74% adoption

The shift to AI-orchestrated SOCs is underway, but adoption without governance creates new risks

Intrusion

AI is weaponized: deepfakes, polymorphic malware, AI phishing

DaaS has democratized attacks

Healthcare's culture of urgency and valuable data makes it uniquely vulnerable

Intelligence

Auditors must evolve: integrate NIST AI RMF, assess AI vendor risks, verify deepfake readiness, and prepare for possible HIPAA Security Rule changes in 2026

Your Action Items

Immediate

Verify MFA is enforced on ALL remote access systems — no exceptions

30 Days

Request a complete inventory of all AI tools deployed in your organization. Identify and classify all ***AI agents*** operating in your environment — treat them as privileged identities requiring Zero Trust controls

60 Days

Conduct a gap assessment against the imminent HIPAA Security Rule final rule — mandatory MFA, AES-256 encryption, and annual pen testing are confirmed requirements

90 Days

Incorporate AI-specific scenarios into your next IR tabletop exercise

Ongoing

Subscribe to Health-ISAC threat intelligence feeds for real-time updates

Polling Question #5

Resources and References

- **Frameworks and Standards**
  - NIST CSF 2.0; nist.gov/cyberframework
  - NIST AI RMF 1.0; nist.gov/itl/ai-risk-management-framework
  - HHS Cybersecurity Performance Goals; hhs.gov/cybersecurity
  - HSCC AI Cybersecurity Guidance (2026); healthsectorcouncil.org
  - Proposed HIPAA Security Rule; Federal Register, Jan 6, 2025
  - NIST AI RMF Generative AI Profile (NIST-AI-600-1); nist.gov
  - NIST Post-Quantum Cryptography Standards (FIPS 203/204/205); nist.gov
  - NIST AI RMF Profile: Trustworthy AI in Critical Infrastructure (April 2026); nist.gov
  - HSCC AI Cybersecurity Governance Guide (June 2026); healthsectorcouncil.org
- **Threat Intelligence**
  - Health-ISAC; health-isac.org
  - CISA Healthcare Advisories; cisa.gov/healthcare
  - HIPAA Journal Breach Reports; hipaajournal.com
  - HHS HC3 (Health Sector Cybersecurity Coordination Center)

- **Key Reports Cited**
  - Proofpoint-Ponemon, "Cyber Insecurity in Healthcare" (2025)
  - SANS/Anvilogic, "Detection Engineering Survey" (2025)
  - CrowdStrike, "Healthcare Cybersecurity in 2025"
  - Seceon, "The 2025 Healthcare Cyber Crisis: $10.3M Breaches"
  - HIPAA Journal, "Largest Healthcare Data Breaches of 2025"
  - Ogletree Deakins, "Healthcare Employers in 2026" (Dec 2025)
  - Verizon 2025 Data Breach Investigations Report (1,710 healthcare incidents)
  - IBM Cost of a Data Breach Report 2025 ($7.42M healthcare avg.)
  - JMIR: "Emerging Risks of AI-to-AI Interactions in Health Care" (March 2026)
  - M-Trends 2026 / Mandiant AI Risk & Resilience Report (Google Security, April 2026)
- **Executive & Legislative**
  - Healthcare Cybersecurity Act of 2025
  - EO 14179, EO 14355, EO 14365,EO 14409, NSPM-11
  - "Advancing Artificial Intelligence Education for American Youth"
  - "Accelerating Federal Permitting of Data Center Infrastructure"
  - "Preventing Woke AI in the Federal Government"

A national healthcare advisory services firm providing consulting, audit, and tax services

PYA by the Numbers

56% FEMALE OWNERSHIP

Over 2x the average of similarly sized firms

- Inside Public Accounting

CLIENT LOCATIONS

INSIDE public accounting TOP 100 FIRMS 2025

accountingTODAY 2025 Top 100 Firms

1500
Healthcare valuation opinions requested annually

OVER **450**
Commercial Reasonableness Arrangements in the last 5 years

USA TODAY
AMERICA'S MOST RECOMMENDED TAX FIRMS
2025 IN COOPERATION WITH statista

TOP **15** LARGEST AUDITOR
of AHA's Top U.S. Multi-Hospital Systems
- Ames Research Group

Modern Healthcare 2025
Largest Healthcare Management Consulting Firms

MORE THAN **2700** HEALTHCARE CLIENTS

Academic Medical Centers | Accountable Care Organizations Ambulatory Surgery Centers | Blood Centers | Clinically Integrated Networks | County Owned Hospitals | Critical Access Hospitals Diagnostic Centers | Dialysis Centers | Health Plans | Health Systems | Home Health Agencies | Hospices | Hospitals Independent Practice Associations | Maternity Centers | Medical Groups | Mental Health Centers | Nursing Homes Physician-Hospital Organizations | Physician Practices | Physical Therapy Centers | Psychiatric Hospitals | Rural Health Centers Safety Net Hospitals | Surgery Centers | Urgent Care Centers

Vision Beyond the Numbers™

We measure our success based on the success of our clients.

Our culture of HELP and helpfulness is an intrinsic daily philosophy.

RESPONSIVE

ACCESSIBLE

COMMITTED

How can we help?