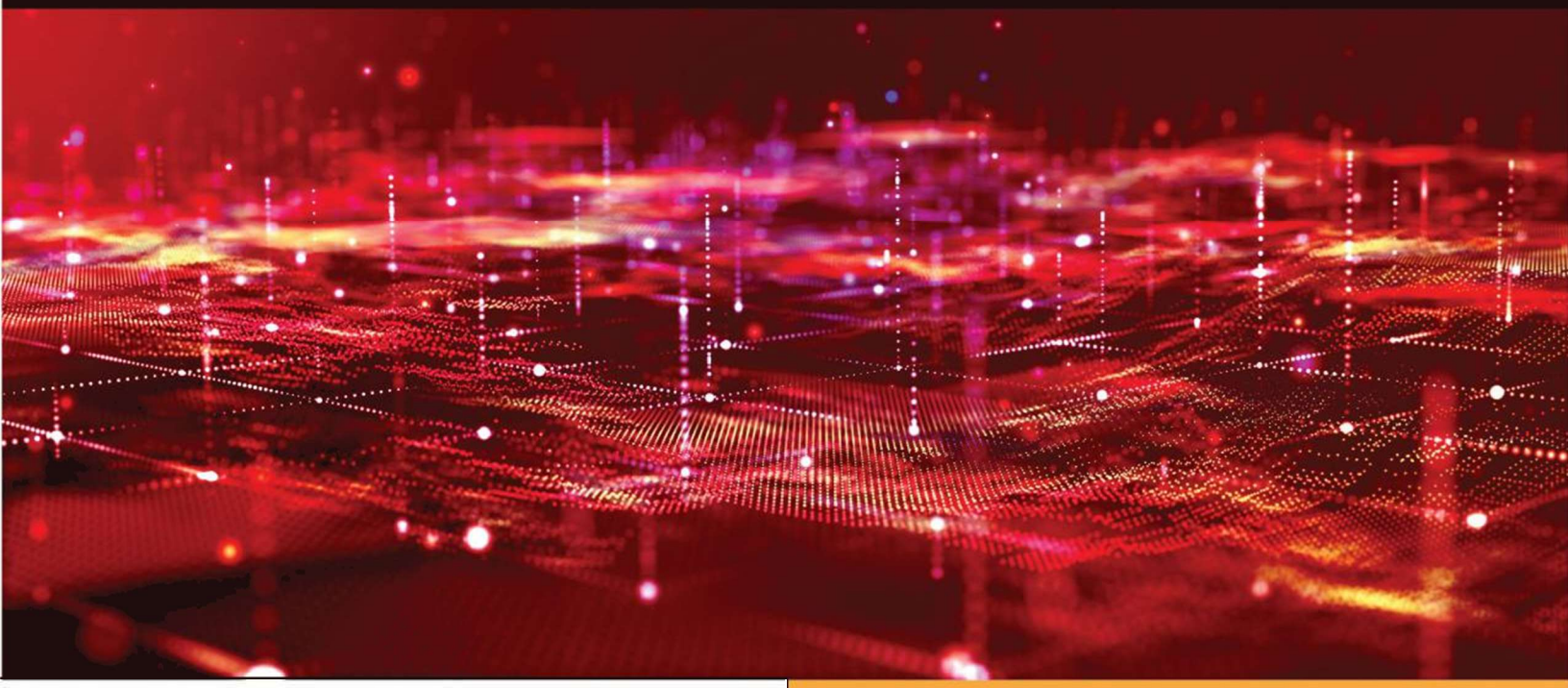
Generative Artificial Intelligence in Healthcare Internal Audit:



ahia

Assoc of Healthcare Internal Auditors

Generative Artificial Intelligence in Healthcare Internal Audit: A Practical Guide

1. Introduction

Purpose and Audience

The rapid advancement of artificial intelligence ("AI") is transforming how businesses operate. Among these innovations, generative AI ("GenAI") stands out for its potential to reshape the audit process, influencing how auditors plan and perform their work.

This guide provides internal auditors in healthcare organizations with practical knowledge and professional guidance on understanding, evaluating, and using GenAI responsibly both (a) in the audit process, and (b) throughout the organization. It is designed to help auditors enhance their efficiency, analytical capability, and strategic insight while maintaining compliance with your organization's policies and procedures, professional standards and regulatory requirements.

This guide focuses on GenAI technologies, which create new content, such as text, code, and images, by learning patterns from large data sets, and their implications for internal audit and the organization. It is not intended to provide technical training on AI development or model validation but rather to build the auditor's capacity to evaluate and apply AI responsibly within the audit function.

Note: The use of generative AI tools should be limited to technologies approved by your organization and must comply with applicable data governance, acceptable use policies, and regulatory requirements (e.g., HIPAA).

How to Use This Guide

Each section provides foundational knowledge, practical applications, and guidance on ethical and governance considerations.

- **Sections 2–3:** Explain foundational AI concepts.
- **Sections 4–5:** Applying the concepts to healthcare auditing.
- **Sections 6–7:** Outline governance, best practices, and future directions.
- **Section 8:** Answers FAQs and provides practical resources.

Why GenAI Matters to Internal Audit

GenAI is transforming healthcare operations, from patient billing and clinical documentation to cybersecurity and compliance monitoring. As organizations leverage GenAI capabilities in their existing systems or develop their own GenAI into core systems, internal auditors must assess both the controls around these tools and their own use of GenAI to enhance audit delivery. A sound understanding of GenAI enables auditors to provide more relevant and timely assurance over emerging risks, governance frameworks, and ethical use of technology.

2. Understanding GenAI: The Basics

What Is GenAI?

GenAI refers to a system of algorithms or computer processes that can create new content, such as text, images, audio, or code, based on patterns learned from large datasets. Unlike traditional programs that follow fixed rules, GenAI uses machine learning to produce context-aware and original outputs.

In healthcare, GenAI may help draft clinical documentation, summarize patient interactions, translate notes, or develop educational materials.

For internal auditors, these same capabilities can be utilized to streamline work such as drafting audit narratives, summarizing evidence, and analyzing qualitative and quantitative data.

How GenAI Works (High Level)

GenAI is powered by Large Language Models (LLMs) that are trained on large datasets through machine learning. They analyze relationships between words, phrases, and concepts to predict the next logical output. For example, when an auditor prompts an AI model to "summarize recent Office of Inspector General (OIG) guidance on billing compliance," it draws on prior text patterns to produce a coherent summary. Think of it as a very advanced form of autocomplete; it does not "think" or "know" facts, but it is skilled at predicting what text should come next based on patterns it has seen before.

However, because LLMs generate responses based on probability rather than verified facts, they can be wrong or misleading (e.g., hallucinations). As such, auditor judgment (e.g., 'human in the loop'), professional skepticism, and verification are **always** required.

The Importance of Prompts

Prompts are crucial in GenAI because they are the instructions input by users to guide the AI to produce relevant, accurate, and high-quality outputs, essentially unlocking the model's potential; better prompts lead to better results by setting context, defining style, and specifying details, saving time and reducing irrelevant or fabricated content. Effective prompts act as the bridge between a user's intent and the AI's capabilities, ensuring the generated text, images, or code meet specific needs, from simple summaries to complex creative tasks.

How It Differs from Traditional AI, Agentic AI, and Audit Analytics

Traditional AI and audit analytics primarily focus on analyzing structured data, detecting patterns, predicting outcomes, or identifying anomalies based on predefined rules or historical trends. Common audit use cases include detecting duplicate claims, predicting patient volumes, or flagging billing exceptions.

GenAI, by contrast, creates new content from unstructured data such as text, emails, policies, or reports. It is well-suited for summarizing documents, drafting audit deliverables, synthesizing large volumes of qualitative information, or generating insights during planning and reporting.

Agentic AI represents a more advanced evolution of GenAI. Rather than responding to a single prompt, agentic systems are designed to autonomously plan, sequence, and execute multi-step tasks within defined boundaries. An agentic AI can decide what to do next, interact

with multiple tools or data sources, and adjust its actions based on intermediate results, while still operating under human-defined rules and oversight.

Type of AI/Tool	Purpose	Example in Audit Work
Traditional AI	Designed to detect patterns, classify data, and make predictions based on historical trends and structured datasets.	Predict claim denials or identify anomalies in billing data using historical transaction patterns.
Audit Analytics	Focuses on evaluating existing data to identify exceptions, control gaps, or trends using rules, queries, and visualizations.	Identify duplicate vendor payments, unmatched transactions, or unusual variances in account balances.
GenAI	Capable of creating new text, summaries, or recommendations based on learned patterns from large datasets.	Draft audit reports, summarize interview notes, or brainstorm emerging risk themes during audit planning.
Agentic AI	Designed to autonomously plan and carry out multi-step tasks, make decisions within defined constraints, and coordinate actions across systems or tools.	Assists with audit planning by gathering background documents, summarizing prior audit results, identifying relevant risks, and proposing a draft audit plan for auditor review.

While traditional AI functions as an efficient analyst and GenAI serves as a creative, contextual partner, agentic AI acts as a proactive assistant capable of planning and executing multi-step tasks to further enhance audit efficiency. Together, these technologies can amplify audit analytics by accelerating planning, analysis, and documentation; however, increasing autonomy also demands heightened professional judgment and oversight. By understanding these distinctions, auditors can better determine when agentic and GenAI appropriately complement traditional analytics, and when their use introduces additional risks such as bias, misinformation (e.g., hallucinations), unintended actions, or data confidentiality concerns.

Example: AI in Action

An internal audit department receives over 300 policy documents during an engagement on revenue integrity. By using an approved GenAI tool, auditors summarize the documents by topic and identify overlapping or outdated policies. This reduces manual review time from weeks to days, while auditors retain responsibility for verifying each summary's accuracy.

Common Tools & Platforms[1]

Developer	Open AI	Anthropic	Google	Microsoft	Various vendors
Platform	ChatGPT	Claude	Gemini	Copilot	Domain-Specific AI Tools

1 Check your organization's policies, procedures and responsible and ethical use standards/guidelines for AI usage.

3. Core Concepts and Key Terms for Auditors

Internal auditors do not need to be data scientists, but familiarity with key AI concepts can enable them to assess the reliability, risks, and control implications of GenAI systems. The following terms highlight common risk areas relevant to both evaluating and using AI tools.

Hallucinations

AI can produce statements that appear credible but are incorrect. These errors occur when the model lacks sufficient context or is trained on incomplete or inaccurate data. Auditors must independently confirm AI-generated information before relying on it as audit evidence.

Human in the Loop (HITL) [2]

Human-in-the-loop (HITL) refers to a system or process in which a human actively participates in the operation, supervision or decision-making of an automated system. In the context of AI, HITL means that humans are involved at some point in the AI workflow to ensure accuracy, safety, accountability or ethical decision-making.

Training Data Quality

The reliability of AI outputs depends heavily on the data used during model training. Data that is biased, incomplete, or outdated can lead to inaccurate conclusions. For auditors, this means assessing whether management understands and validates data sources underlying AI systems.

Bias

AI models can replicate or amplify societal, demographic, or procedural biases present in training data. In healthcare, this may result in uneven treatment recommendations, inequitable billing patterns, or flawed decision rules. Internal auditors should evaluate whether bias understanding, testing and monitoring are part of management's AI governance processes.

Transparency and Explainability

AI systems often function as "black boxes," producing results without clear insight into how conclusions were reached. Lack of transparency creates challenges for both management accountability and audit validation. Auditors should determine whether AI models used by the organization are explainable, documented, and reproducible.

Data Privacy and Leakage

Information entered into an external AI system may be retained or processed by third parties. Inputting Protected Health Information (PHI), Personally Identifiable Information (PII), or proprietary data into public tools can violate HIPAA and organizational confidentiality obligations. Auditors must confirm that only secure, organization approved systems are used for sensitive and confidential data.

Operational and Business Risks

The proliferation of GenAI can introduce new and amplify existing operational and business risks such as over-reliance on outputs without appropriate checks and balances, creation of realistic fake information for fraudulent purposes, system vulnerabilities from new entry points for attackers, and violations of legal and regulatory requirements.

---

[2] What is human-in-the-loop?, Cole Stryker, Staff Editor, AI Models IBM Think

Accountability and Governance

Organizational expectations for the accountability and governance of AI center on establishing clear, human-centric frameworks guided by core principles: accountability, transparency and explainability, fairness and bias mitigation, privacy and security, and reliability and safety. These expectations are driven by the need to mitigate significant risks, ensure regulatory compliance, and build trust among stakeholders.

AI initiatives require clear ownership for decision-making, performance, and outcomes.

Internal auditors should assess whether the organization's AI governance program defines roles, responsibilities, and escalation protocols.

4. Applying GenAI in Healthcare Internal Audit

The Changing Healthcare Audit Environment

Healthcare organizations are adopting AI for administrative efficiency, diagnostics, and decision support. Internal audit must evolve in parallel, moving from manual analysis toward technology-enabled assurance. In addition, as organizations expand their use and reliance upon these new technologies, Internal Audit must take an active role in understanding and evaluating risks and controls associated with its adoption.

The Auditor's Role

Internal auditors serve as evaluators of AI risks and as responsible users of AI within their own processes. This dual role requires balancing innovation with critical thinking, professional judgement and skepticism, adherence to governance expectations (e.g., policies, procedures, internal controls, and training) and industry and ethical standards.

Internal audit functions investing in GenAI enabled tools expect such tools to augment, but not replace, auditors in the audit process. Auditors who utilize these tools are still responsible for the results and documentation of the work. Policies for supervision and review remain a critical part of audit quality assurance.

Examples of Where GenAI Adds Value

Risk Identification and Prioritization:

AI can analyze large amounts of data to identify potential risks (known and unknown) and assess their impact, likelihood and velocity on an organization.

Example: Using AI provides data supported insights allowing organizations to proactively identify risks and make well-informed decisions.

Planning:

AI can accelerate background research, summarize regulatory updates, and assist in drafting audit objectives or risk matrices.

Example: Using AI to analyze recent OIG or Centers for Medicare & Medicaid Services (CMS) publications to identify emerging risk themes.

Fieldwork and Testing:

AI tools can summarize policies, extract themes from interviews, generate initial control listings, review contracts, draft initial testing templates or sample selection criteria, or identify

patterns or anomalies in large datasets. Auditors must still validate accuracy and document reliance levels.

Example: In a review of collection agency recoveries, AI summarizes monthly reports, highlighting discrepancies in reported versus posted recoveries for further testing.

Root Cause Analysis:

AI tools can group similar issue types together, highlighting possible root causes. Auditors must validate the accuracy of such root causes.

Example: A review of training transcripts may reveal gaps in key elements and/or stakeholders.

Reporting:

GenAI can support the preliminary drafting of observations, executive summaries, or formatting of reports, freeing auditors to focus on analysis and recommendations.

Note: *AI-generated drafts save time but should be reviewed carefully to ensure factual accuracy and alignment with professional tone and judgment.*

Continuous Monitoring:

AI can identify anomalies or patterns in large datasets for early risk detection, enhancing ongoing assurance and follow-up reviews.

Any use, step taken to validate, and reliance on AI should be documented by auditors in all phases of an engagement.

5. Risks, Governance, and Ethical Considerations

Operational Risks

AI introduces distinct operational and compliance risks that require careful oversight and validation. It is important to note that existing auditing standards are technology-neutral and apply to the use of AI (e.g., the auditor must be able to understand the basis for their conclusions and audit evidence must allow for reperformance of procedures). AI can introduce new complexities when adhering to these standards. Internal Audit functions must implement appropriate risk management guidance, controls, and supervision of AI tools, including governance, approval, and quality assurance controls, before relying on AI-generated information or using AI tools in audit activities.

Risk Type	Description	Audit Focus
Accuracy	AI may generate incomplete, fabricated, or misleading information.	Verify the accuracy of AI outputs against reliable, authoritative sources (i.e., regulations); require citation or identification of sources where applicable; and document validation and corroboration procedures.
Bias	Outputs may reflect or amplify bias from training data, resulting in discriminatory or inequitable outcomes.	Assess data governance practices, bias detection controls, and model fairness testing.
Privacy	Use of AI tools can inadvertently expose protected or sensitive information.	Evaluate compliance with organizational data protection policies, HIPAA, GDPR and vendor data handling standards.
Transparency	Limited visibility into how AI models and underlying data generate outputs can hinder accountability, auditability, and reperformance.	Review governance frameworks for model documentation, explainability, and decision traceability.
Accountability	Unclear ownership of AI risk or unethical use of tools may lead to control gaps.	Confirm that oversight responsibilities, approval workflows, and ethical use policies are clearly defined and monitored.
Objectivity	Overreliance on AI may impair professional skepticism and auditor judgment.	Reinforce that AI is a tool that supports, not replaces, critical thinking, evidence evaluation, and independent judgment.

Regulatory and Ethical Frameworks

In addition to operational risks, AI use in healthcare and audit functions is subject to a growing set of regulatory and ethical expectations. Internal auditors should understand these frameworks to evaluate whether their organizations, and their own audit practices, align with legal, ethical, and professional standards.

- **HIPAA:** Requires strict protection of PHI. Inputting any identifiable patient information into public AI tools is prohibited.
- **Global Data Protection Regulation (GDPR):** Data and privacy security law that applies to organizations which process EU citizens'/residents' personal data or if goods or services are offered to such individuals.
- **National Institute of Standards and Technology (NIST) AI Risk Management Framework:** Provides principles for trustworthy AI, including transparency, security, and accountability.
- **Global Internal Audit Standards:** Define the principles and requirements for the professional practice of internal auditing worldwide, emphasizing independence, professional judgment, and effective governance and risk management, including the responsible use of emerging technologies such as AI.
- **OIG Compliance Program Guidance:** Encourages oversight of technology use in healthcare operations and supports internal audit's role in evaluating system controls.

Balancing Innovation and Accountability

AI offers efficiency and analytical benefits, but its adoption must be governed through well-defined frameworks that clearly establish the following elements:

- Establish an oversight body and define roles and responsibilities for AI risk management throughout the organization.
- Develop clear policies outlining acceptable AI use cases, privacy and security guidelines, data handling procedures, and ethical standards.
- Conduct comprehensive and ongoing risk assessments to identify technical, ethical, operational, and reputation risks and conduct regular audits of AI systems for performance, compliance, and model drift.
- Align internal practices with recognized frameworks.
- Provide ongoing education and training for employees to build AI literacy and foster a culture of responsible AI use.

Internal auditors should assess whether management has established policies addressing these elements and whether governance bodies receive regular reporting on AI-related risks and performance.

6. Best Practices for Safe and Effective AI Use

The Three Pillars of Responsible Use

1. **Protect Data**
   Safeguard sensitive information, respect privacy, and prevent against attacks or misuse. Never input PHI, PII, or proprietary content into external tools. Use organization-approved and secure platforms.
2. **Validate Outputs**
   Always review AI-generated outputs for accuracy, completeness, and alignment with source information (e.g. 'human in the loop'). Do not rely on AI for final conclusions or audit evidence.
3. **Apply Judgment**
   AI can enhance efficiency but cannot replace professional reasoning. Maintain skepticism and evaluate whether AI-supported work aligns with audit objectives and standards.

Safe Use Principles

- Confirm AI tools are approved and compliant with internal IT and data governance policies.
- Avoid sharing confidential or identifiable data, unless allowable under your organization's policies (e.g., some organizations have Gen AI tools that sit within their network/firewall and can be provided confidential information).
- Cite or footnote when AI-generated content informs audit documentation and audit report findings.
- Maintain version control to show how AI outputs were reviewed or adjusted.
- Provide staff with AI literacy and ethics training.

Documenting and Reviewing AI Use

Auditors should document how AI was applied, including the following:

- The tool used and purpose (e.g., summarization, drafting).
- Validation steps taken.
- Limitations identified.
- Final auditor judgment.

Supervisory review should include an evaluation of AI-related decisions and confirm adherence to professional standards.

Quality Assurance Alignment

AI-assisted work must still comply with the internal audit methodology and quality assurance framework. This includes peer review, documentation traceability, and evidence validation.

AI Audit Readiness Checklist

Before using AI tools, auditors should confirm the following:

- ☐ Confirm IT and compliance approval.
- ☐ Avoid entering confidential or regulated data.
- ☐ Validate and document outputs.
- ☐ Note AI use in audit workpapers.
- ☐ Confirm alignment with IIA Code of Ethics.

7. The Future of AI in Healthcare Auditing

As healthcare organizations continue adopting advanced technologies, generative AI and machine learning will increasingly intersect with audit analytics, compliance, and risk management. Internal auditors must anticipate these changes, adapting their methods, skills, and collaboration practices to remain effective and trusted advisors.

Integration with Audit Analytics

AI will increasingly integrate with existing audit analytics platforms. For example, anomaly detection, process mining, and exception tracking may soon combine with generative tools to automatically produce narrative explanations of data results. Internal audit will shift toward continuous assurance and predictive insight.

Evolving Auditor Skillsets

As AI becomes integral to audit operations, auditors must develop the following capabilities:

- **AI Literacy:** Understanding how models function, their limitations, and validation methods.
- **Data Analytics:** Ability to interpret outputs and detect anomalies.
- **Critical Thinking:** Applying judgment to complex AI-derived insights.
- **Ethical Reasoning:** Recognizing bias and ensuring responsible tool use.

Collaboration Across Functions

Internal audit will work more closely with:

- **Compliance:** Ensuring ethical and regulatory AI use.
- **IT and Cybersecurity:** Evaluating system access, dataflow, and integrity.
- **Data Science:** Understanding algorithms, model validation, and performance metrics.
- **Legal:** Ensuring compliance with federal, state and local laws and regulatory requirements.
- **Risk Management:** Assessing emerging AI risks that may impact organizational performance and AI use.

Cross-functional collaboration enhances audit relevance and governance maturity.

Vision for the AI-Enabled Auditor

The AI-enabled auditor leverages technology to gain efficiency and insight but remains grounded in professional skepticism and ethical standards. Auditors are not replaced by AI, instead they are strengthened by it. Future audit functions will rely on auditors who combine technological fluency with sound judgment and integrity.

8. FAQs and Resources for Auditors

Q1: Can I put Protected Health Information (PHI) into ChatGPT or other public AI tools?

A1: No. Public generative AI tools are not HIPAA-compliant and may store or reuse data. Never input PHI, confidential patient details, or proprietary information. Validate that such information is not used by leveraging strong access controls. Use only enterprise-approved, secure AI platforms that meet your organization's governance and privacy and security standards.

Q2: How do I know if AI's answer or analysis is reliable?

A2: Treat AI output like any unaudited information source, use professional skepticism. Always validate AI-generated insights, summaries, or calculations against authoritative and verifiable sources, such as system reports, policies, or regulatory guidance. Document your verification process.

Q3: What AI tools are safe for auditors to use?

A3: Only use AI tools that are approved, licensed, and compliant with your organization's information security and HIPAA requirements. Check whether the tool has undergone IT risk assessment or vendor due diligence. Avoid personal or experimental AI applications for audit work.

Q4: How should AI-generated work be treated as audit evidence?

A4: AI outputs can support audit work but should not stand alone as evidence. Auditors must take the following actions:

- Corroborate AI results with independent data or documentation.
- Document how AI-supported evidence was verified.
- Treat AI output as supplemental or preliminary analysis, not final proof.

Q5: How should I document AI-assisted work in my audit file?

A5: Clearly identify where and how AI was used. For example:

- Note the AI tool's name, version, and purpose (e.g., summarizing policies, analyzing text).
- Retain evidence of prompts, and verification of AI-generated outputs and supporting sources and/or references.
- Include a brief disclaimer or notation in workpapers, such as "AI-assisted draft reviewed and validated by auditor."

Transparency supports audit quality and regulatory defensibility.

Q6: Could using AI impair independence or objectivity?

A6: If over-relied upon, AI can introduce bias or dependency that affects auditor judgment. Maintain objectivity by doing the following:

- Critically reviewing all AI-assisted analyses and conclusions.
- Exercising final human judgment on audit results.
- Avoiding use of AI tools developed or managed by areas under audit unless approved and controlled.

Q7: What are "AI hallucinations," and why do they matter for auditors?

A7: "Hallucinations" occur when AI generates false or fabricated information that appears credible. For auditors, this presents a significant risk of inaccurate findings or misleading documentation. Always verify all AI-generated facts, figures, or interpretations with source data or authoritative references.

Q8: Will AI eventually replace internal auditors?

A8: No. AI will enhance, not replace audit work. It can automate repetitive tasks and enable deeper analytics, but critical thinking, ethical reasoning, and professional judgment remain irreplaceable. AI is a tool, and auditors remain accountable for conclusions and recommendations.

Q9: What skills should I develop to prepare for AI's impact on auditing?

A9: Focus on building AI literacy and complementary skills such as the following:

- Understanding AI concepts and data governance.
- Strengthening data analysis and visualization capabilities.
- Enhancing critical thinking, communication, and risk assessment in AI contexts.
- Staying informed on regulatory developments affecting AI in healthcare.

Q10: How do regulators (e.g., OIG, CMS, HHS) view AI use in compliance and audit?

A10: Regulators emphasize strong governance, privacy safeguards, and accountability in AI deployment. Expect scrutiny around the following:

- Data handling (HIPAA and cybersecurity compliance).
- Model transparency and bias.
- Audit trail integrity for AI-assisted decision-making.

Internal audit should proactively evaluate whether the organization's AI use aligns with emerging federal guidance and industry best practices.

Q11: Where can I learn more about AI governance and auditing?

A11: Resources include:

- Your Organization's AI Policy: Always your first reference point
- The Institute of Internal Auditors (IIA): *Artificial Intelligence Auditing Framework*
- National Institute of Standards and Technology (NIST): *AI Risk Management Framework (AI RMF 1.0)*
- International Organization for Standardization (ISO): *ISO/IEC 42001: AI Management Systems*
- U.S. Department of Health & Human Services (HHS): *HIPAA and Emerging Technologies Guidance*
- Office of Inspector General (OIG) and Centers for Medicare & Medicaid Services (CMS): Compliance program guidance and emerging AI risk statements
- Office for Civil Rights (OCR): *AI and Data Privacy Considerations*
- IIA Prompt Library

Author: AHIA Gen AI Working Group

Members

- Tania Arruda
- Lisa Berghaus
- Christopher Broome
- Michelle Byers
- Kara Campbell
- Ted Flom
- Julie Garrison
- Darrell Goolsby
- Thayana Hermano
- Grace Kau
- Laura Morgan
- Kelly Rollins
- Shawn Shelley
- Brian Singh
- Amanda Smith
- Evan Webber
- Ryan Willhite
- Colin Stuart-Morse

About AHIA

The Association of Healthcare Internal Auditors (AHIA) is a network of experienced healthcare internal auditing professionals who come together to share tools, knowledge, and insight on how to assess and evaluate risk within a complex and dynamic healthcare environment. AHIA is an advocate for the profession, continuing to elevate and champion the strategic importance of healthcare internal auditors with executive management and the Board. If you have a stake in healthcare governance, risk management and internal controls, AHIA is your one-stop resource. Explore our website for more information. If you are not a member, please join our network, www.ahia.org. AHIA white papers provide healthcare internal audit practitioners with non-mandatory professional guidance on important topics. By providing healthcare specific information and education, white papers can help practitioners evaluate risks, develop priorities, and design audit approaches. It is meant to help readers understand an issue, solve a problem, or make a decision. AHIA welcomes papers aimed at beginner to expert level practitioners. This includes original content clearly related to healthcare internal auditing that does not promote commercial products or services. **Interested? Contact a member of the AHIA White Paper Subcommittee.**

Subcommittee:

Valerie Mattas, White Paper
Chair
Sharp Healthcare
valerie.mattas@sharp.com

Alan Henton
Vanderbilt University Medical Center
alan.p.henton@vumc.org

Debi Weatherford
Piedmont Healthcare
debi.weatherford@piedmont.org

Laura L. Sak-Castellano
Advocate Aurora Health
Laura.Sak-Castellano@aah.org

Deborah Pazourek, AHIA Board Liaison
MedStar Health
Deborah.L.Pazourek@medstar.net