hfma ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

HFMA/NEHIA

2026 Compliance & Internal Audit Conference

Artificial Intelligence: Evolving Compliance and Privacy Challenges and Practical Use Cases

Wednesday, December 2 - Friday, December 4, 2026
Mystic Marriott Hotel, Groton, CT

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

hfma ma-ri chapter

HFMA/NEHIA

2026 Compliance & Internal Audit Conference

Artificial Intelligence: Evolving Compliance and Privacy Challenges and Practical Use Cases

Wednesday, December 2 - Friday, December 4, 2026
Mystic Marriott Hotel, Groton, CT

Objective and Agenda

This panel presentation will focus on practical AI use cases for Compliance and Privacy professionals:

- Privacy risks and use cases, including shadow AI, third-party risk, and proactive use of agents
- AI for compliance monitoring
- Developing an AI policy (key terms, launching & training)
- Conducting better/faster regulatory research with AI
- Governance to evaluate vendors
- Using AI to create tools to manage conflicts of interest

hfma ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

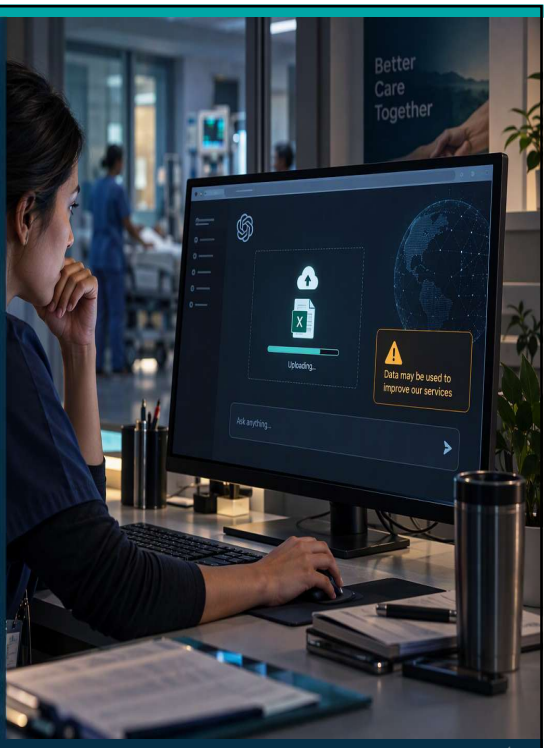
ONE UPLOAD.

3,182 PATIENTS NOTIFIED.

A Johns Hopkins workforce member uploaded a spreadsheet containing patient information to a public AI tool that had not been approved for that use.

THAT IS SHADOW AI.

Reported incident, September 2026 • Public reporting did not identify the AI tool.



SHADOW AI + GOVERNANCE

SHADOW

GOV

SHADOW AI

43%

Security incidents involving shadow AI, up from 20% in 2025

GOVERNANCE GAP

68%

Breached organizations that lacked AI governance to manage AI or detect shadow AI

Source: IBM Cost of a Data Breach Report 2026

Shadow AI turns a helpful shortcut into a privacy event

The risk begins when protected information leaves approved systems and organizational controls.

1 APPROVED SYSTEM

Access controls, monitoring, policies and approved workflows protect patient information.

2 UNAPPROVED AI

A user copies or uploads data to solve a legitimate business problem faster.

3 EXTERNAL PROVIDER

Retention, secondary use, deletion and downstream access may be unclear or uncontrolled.

4 ORGANIZATIONAL IMPACT

Investigation, notification, remediation, patient concern and loss of trust.

The practical control is not “just say no.”

MAKE THE SAFE PATH EASY

Provide approved enterprise tools and clear “yes” use cases.

TEACH THE BOUNDARY

Do not enter patient, employee, privileged or confidential information into unapproved tools.

BUILD VISIBILITY

Use governance, vendor review, access controls, monitoring and incident response together.

AI for Compliance Monitoring

- AI monitoring tools for shadow AI
- After deployment what does monitoring look like?
  - Monitoring for drift
  - Monitoring for bias
  - Monitoring for hallucinations
  - Monitoring for performance

hfma ma-ri chapter

Launching, Implementing & Revising an AI policy

- **Overall Thought**: Because AI scales benefits and scales risks, let's proceed and pursue value-adding new technologies with a **good process** that includes management governance, cross-functional participation, and appropriate controls.
- **Key Concepts**: (1) No sensitive data in unapproved tools, (2) users accountable for outputs, (3) HIPAA still applies (min. necessary, BAAs, deidentification), (4) address data rights/protection in contracts, and (5) provide guidance re: specific uses: clinical, AI transcripts and notes
- **Launching the policy**:
  - **Training**: Initial education (quiz at launch) and annual education thereafter. Can use access to a tool as a "carrot" – must complete training for access.
  - **Review sessions**: Review policy with key stakeholder groups to raise awareness, e.g., re: review of vendor products, including need to review new AI functionalities offered by existing customers.
  - **Email channel for questions**: Create a "Responsible AI" email alias
- **Post-launch Communications**
  - Describe and announce the "yes" use cases.
  - Reinforce not entering patient/sensitive data into personal (unapproved) AI tools. Put the focus on safer enterprise tools (where available).

hfma ma-ri chapter

Conducting better/faster regulatory research with AI

Practical recommendations:

- Use an enterprise model with contractual protections and a business associate agreement.
- Be mindful of inputs with potentially privileged or sensitive information.
- Describe your goal and ask the tool for help developing a prompt.
- Provide Role, Task, and Context
- LLMs are probabilistic - ground the AI:
  - Tell the AI to review a "golden" example of what you want an output to look like.
  - Use Copilot "Notebooks" to store instructions, references, and golden examples.
- Save your best prompts and continue to improve them as you learn more.
- Value of crowdsourcing. Share what worked/didn't work, and concerns.

hfma ma-ri chapter

Governance to evaluate vendors - Tips

- **Key Concepts**: (1) employ a cross-functional approach to effectively manage; (2) ask questions – conduct active vendor due diligence; (3) leverage existing processes and control approaches (auditing/monitoring); (4) protect your data.
- **Conducting Evaluations --** Responsible AI Committee or similar group can:
  - Develop and use the same evaluation rubric each time;
  - Identify the owner;
  - Identify the "why", e.g., what problem are we solving, why now, and what happens if we do nothing?;
  - Develop a menu of standard responses and controls to build consistency and speed the process;
  - Partner with stakeholders re: what type of validation is appropriate for a particular AI functionality
  - Discuss how a human will stay in the loop (with increasing automation)
  - Make the completed rubrics easy to find to help draft the next ones. Many AI functionalities are similar.
- **Contracting**:
  - Consider collaborating with Legal re: an AI addendum of key contractual terms (data rights, indemnification) and business associate agreement terms.
  - Be mindful – existing vendors may introduce new AI functionalities
- **Following up**:
  - With AI, the process needs to be **ongoing**.
  - Create a calendar to keep track, e.g., of when owners will report back to the Committee or set up a quarterly meeting to touch base on the products (like ambient).

hfma ma-ri chapter

Developing COI Management Plans



hfma ma-ri chapter

COI Questionnaire

01 :Is the researcher a cofounder in a company outside of BCH?

select

02 :What is the researcher's role(s)/title(s) in the company?

Founder, Director

03 : Is the company publicly traded or privately held?

select

04 : What is the researcher's equity in the company?

05 : How much will the researcher be compensated in cash from the company annually?

select

06 : How much time/effort does the researcher spend working for the company?

select

07 : Has the company licensed or is it planning to license intellectual property from BCH?

select

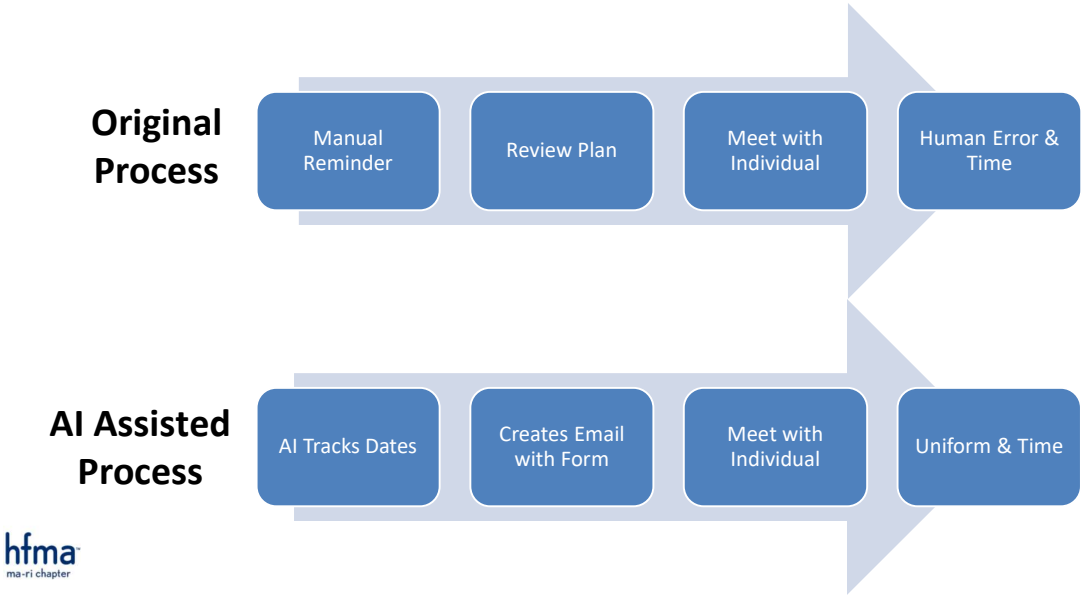
hfma ma-ri chapter

Scoring Report

User Input	PDF Data	Status	Weight/Score
Yes	Yes	✓ Match (Exact)	3.0 / 3.0
Founder, Consultant	Co-founder,Consultant	✓ Partial Match (Overlap: 2 tokens)	2.4000000000000004 / 3.0
HMS_COI_Policy	HMS_COI_Policy	✓ Match (Exact)	3.0 / 3.0
[Research Support Rule (formerly the "1(b) Rule")]	Research Support Rule (formerly the "1(b) Rule")	✓ Match (Exact)	3.0 / 3.0
Yes	Yes	✓ Match (Exact)	3.0 / 3.0
Private	Private	✓ Match (Exact)	1.0 / 1.0
[Cash, Stock]	Stock	✓ Partial Match (Overlap: 1 tokens)	0.8 / 1.0
≤ 20 %	≤ 20 %	✓ Match (Exact)	1.0 / 1.0
Yes	Yes	✓ Match (Exact)	1.0 / 1.0
Basic	Basic	✓ Match (Exact)	1.0 / 1.0
No	No	✓ Match (Exact)	1.0 / 1.0
Yes	Yes	✓ Match (Exact)	1.0 / 1.0
No	Yes	✕ Mismatch	0.0 / 1.0
≤ $ 25000	NA	✕ Mismatch	0.0 / 1.0
Yes	NA	✕ Mismatch	0.0 / 1.0

hfma ma-ri chapter

Auditing COI Management Plans



hfma ma-ri chapter

Questions

hfma ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

Appendix

hfma ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

Ground the AI – Role, Task, Context: Privacy Research Example

Role:

- Your role is to serve as a health care privacy professional who will explain an issue and provide a useful and practical response to another health care privacy professional

Task:

- Consult the sources I've identified.
- Provide a response that (1) includes an executive summary at the top; (2) uses numbered sections and bullets; (3) is reasonably concise and executive friendly, (4) provides links to sources materials; (5) labels what the text says versus your synthesis/analysis
- Ask me questions at the end to help to tailor and improve the quality and accuracy of the response.

hfma ma-ri chapter

Ground the AI – Role, Task, Context for Privacy Research

Context:

- **Overall**: Health care industry, particularly hospitals, physicians, home health, and hospice
- **Your Company**: For my company, see the document in the references titled, "[System Name] Background Information."
  - In this document, you can, e.g., identify your entities (types, locations), indicate which are covered entities/business associates, identify any Part 2 entities that are subject to Part 2 (SUD).
- **Sources**: Provide a list of sources with cites and links to HIPAA regulations and HHS HIPAA guidance.

hfma ma-ri chapter

Copilot's recent advice to me re: accuracy

Include in prompt:

- Accuracy is more important than speed or brevity.
- Before answering, independently check the proposed conclusion against the available source material.
- Verify all material facts, citations, quotations, dates, numbers, names, and current-status statements.
- Distinguish clearly among: (1) facts directly supported by a source; (2) reasonable interpretations; (3) assumptions; and (4) recommendations.
- Identify conflicting authority, material exceptions, missing information, and uncertainty.
- Do not fill gaps with plausible-sounding information.
- If a point cannot be verified, say so explicitly.
- Before finalizing, perform a completeness and consistency check and correct any unsupported or contradictory statements.
- Cite the source supporting each material conclusion.

hfma ma-ri chapter