hfma™
ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

HFMA/NEHIA

2025 Compliance & Internal Audit Conference

Wednesday, December 3 - Friday, December 5, 2025
Mystic Marriott Hotel, Groton, CT

TuftsMedicine

HFMA / NEHIA Joint 2025 Compliance & Internal Audit Conference

CCO Perspectives on Artificial Intelligence: Regulatory Issue Spotting, Best Practices for Governance and Controls & Vendor Selection and Management

Garrett Gillespie, Chief Compliance Officer, Tufts Medicine

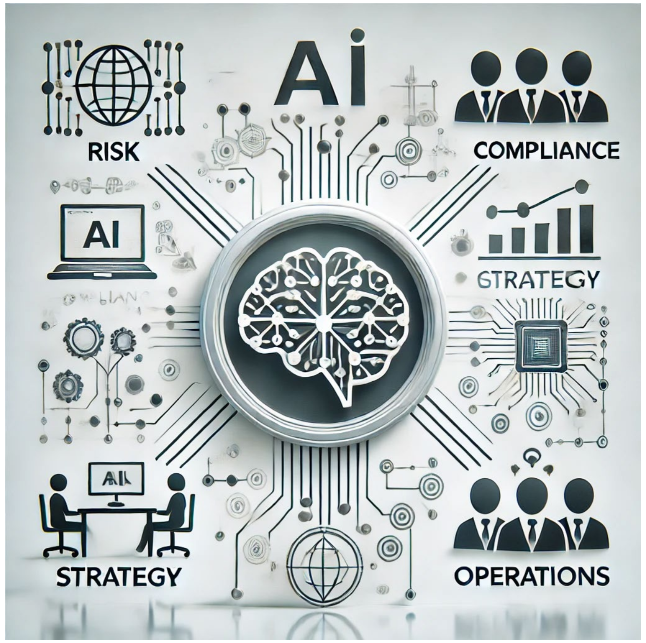
December 5, 2025

Artificial Intelligence – CCO Perspective: Issue Spotting, Governance, Controls, Vendor Management

- Recommended overall approach to AI: balance enthusiasm with prudence
- AI issue spotting for Healthcare Entities
- Establishing Initial AI Governance and Controls:
  - AI Use Policy
  - Responsible AI Committee
  - AI Strategy Committee
  - AI Product and Vendor Management

Balance Enthusiasm with Prudence

- **Key takeaway: AI scales benefits <u>and</u> scales risks**
- Let's proceed and pursue value-adding new technologies…
- **<u>with</u>** a **good process** that includes management governance, **cross-functional participation**, and appropriate controls,
- *And let's be humble and curious about what we don't know.*



- **Demis Hassabis, CEO and co-founder of Google DeepMind**: "I'm **optimistic** that we'll get this right, **as long as we approach it in the right way**, actually, using the scientific method and trying to be very thoughtful about each step that we take[.]"

AI Issue Spotting for Healthcare Entities

- **AI-specific laws, regulation & guidance:**
  - **Legislation/regulation**: states and federal agencies have taken the lead so far on legislation and regulatory guidance.
  - **Focus so far**: medical device requirements, consumer protection, accuracy of product claims, bias & discrimination, transparency, utilization management (CMS), use in employment.
- **Billing and coding**: if the product could impact billing, need to validate accuracy.
- **Contracts**: address who bears what risks, study the warranties and reps re: product.
- **Data rights/privacy**: consider who owns the data, how will it be used.
- **FDA device requirements:** understand what the intended uses of the product are, and whether the product might evolve.

AI Issue Spotting for Healthcare Entities, cont.

- **Governance & decision-making:** need structure and process.
- **Healthcare regulations and AI**: issues include: corporate practice, medical board licensure and discipline, telehealth & AI (both have state-by-state regulation)
- **IP**: consider who owns the product, product improvements, and the outputs. Be mindful of user agreements (and how they can change).
- **Liability & insurance**: consider both the organization and practitioners.
- **Quality processes**: for manufacturers, but customers should consider:
  - Protocols, controls, documentation,
  - Human-in-the-loop,
  - Auditing and monitoring (pre-launch, pilots, **post-launch**),
  - Reporting & quality feedback loops
- **Security**: cybersecurity controls

Establishing Initial AI Governance and Controls

Key Concepts:

- Just start.
- We don’t have to be perfect to be good, and good is a lot better than nothing.

First elements:

- AI Use Policy
- Responsible AI Committee
- AI Strategy Committee
- AI Product and Vendor Management

AI Acceptable Use Policy

- **Just start**: publish a B+ policy with key concepts *now* versus waiting a several months to develop an A+ policy.
- **Key concepts to include**:
  - Users are (1) responsible for not inappropriately inputting sensitive data and (2) accountable for outputs and verifying their accuracy.
  - Privacy and security rules still apply (no AI HIPAA exception): Minimum necessary, business associate agreements, proper de-identification.
  - Contracting: set a mechanism for review & approval of AI products, watch out for who has data rights and whether vendor seeks to train its model with your PHI.
  - Specific uses to address in the policy: e.g., clinical use, LLMs, AI meeting transcription tools/bots.

Responsible AI Committee

- **Get-stuff-done group**: Assemble a small group of subject matter experts (SMEs) who can quickly assess and take action.
- **Key components**:
  - **The who**:
    - Should be collaborative, practical, cross-functional leaders who can think strategically.
    - Consider IT (cyber, applications), clinical (CMIO), compliance (controls, process), and Risk. Depending on your team, can include or consult an AI SME and Legal.
  - **The what (first charge)**:
    - Evaluate and make decisions (tactical) regarding proposed AI product/functionalities.
    - Implement initial controls.
  - **Reporting**: Develop a reporting cadence to key senior leaders and AI Strategy Committee.

AI Strategy Committee

- **Strategy & decision-making group**: senior leaders who can set strategy and make decisions (big picture, material) for the organization, including:
  - Focus: what are the key problems to solve?
  - Costs, benefits, and resources
  - Build or buy? If buy, pursue a potential JV/partnership (with, e.g., economic participation), or a standard vendor engagement.
  - IP commercialization.
- Support thoughtful and efficient organizational decision-making by evaluating and **funneling** the best innovative-technology proposals to senior decision makers.
- Guide and support the development of appropriate controls and confirm their implementation
- Assign tasks to Responsible AI Committee and receive reports.

Examples of AI controls for Ambient AI: Pilot with initial auditing & follow-up monitoring

- **Data**: understand and test the security, data collection, use, storage, and access. Leverage existing security risk assessment process.
- **Auditing and monitoring**: conduct a pilot and initial audit of the product's performance, including its accuracy, reliability, and safety:
  - Before broad launch, evaluate product re: e.g., clinical impact & documentation and revenue/expense/billing impact. Tailor audit to the product.
  - Monitor and test products ***post*** launch for continuous learning and adaptation.
- **Consent**: create processes to obtain and manage consents, where appropriate.
- **Policy**: describe how AI can be used & product-approval processes.
- **User training:** educate and reinforce controls.

AI Product and Vendor Management: Governance mechanisms

- **Proactive**: Develop a process to seek out the AI products that will solve the problems you identified.
- **Reactive**: Create an intake mechanism (**single pipe**) for internal requests to use AI products and vendor proposals. May be able to leverage existing IT processes such as request forms and portals.
- **Approval process**:
  - Develop written criteria to uniformly assess and approve AI vendors and products. Document and retain your evaluations.
  - Process could flow through an existing IT tool with the addition of an AI-specific addendum.
  - Create and share a list of already-approved vendors and their functionalities (save time, manage the total volume of vendors).

AI Creep

- AI functionality can come in through the **front door**, such as when we purchase a new, AI-specific product
- Or it might “creep” in through a side **window or the back door**, such as when an existing product we’ve purchased **adds** AI functionality (Epic, Workday).
- The key variable isn’t whether the **product** or **vendor** is new, it’s whether the **functionality** is new and novel to the extent that we want to have a thoughtful process to consider its potential purchase and implementation.

Contract to protect privacy & data rights

- What data will the vendor need?
  - Will deidentified data suffice?
  - If not, consider minimum necessary
- How will your organization allow the vendor to use the data?
  - Make a conscious decision re: whether and how you will allow the vendor to use your organization’s data to improve its product/model.
- With your Legal team, read the MSA, SOW, and BAA closely re: privacy-law compliance, data rights, and indemnification.
  - Press for what your organization needs.
- Protect your organization’s privacy and business interests.

Understand vendor ROI projections

- Decisions re: whether to select a product may be impacted by vendor ROI projections.
- These projections may be based on a combination of:
  - **Client-specific factual inputs**: how many beds do you have, how many lives, markets/regions served, payer mix, etc.;
  - **Product experience**: the ROI data from previous clients; and
  - **Assumptions (imputed ROI)**: vendor may embed assumptions in the projection, e.g., results from a study or other sources.
- To assess the accuracy of the project, ask – **“What are all the factual inputs, actual experience, and assumptions that you used to create the ROI projection?”**
- Understand **all** the elements of the calculation so your organization can perform a reasonable assessment.

AI Product and Vendor Management: Key Takeaways

- Employ a **cross-functional approach** to effectively manage.
- **Ask questions** – conduct active vendor due diligence.
- **Leverage** existing processes and control approaches (auditing/monitoring).
- **Protect** your data.
- **Standard vendor management concepts still apply**:
  - Keep a **human-in-the-loop** (with increasing automation)
  - **Track performance**: performance guarantees, service line agreements, ROI projections, auditing & monitoring.
- **Be humble and learn** – challenge for all of us: to properly enable, protect, and manage risk for our organizations, we must:
  - **Understand** – to the best extent that we can – how AI products work and the issues they present; and
  - **Share** best practices with each other.

TuftsMedicine

Questions?

TuftsMedicine

Appendix

First – consider these key business questions

Ask:

- What problems are we trying to solve?
- Build or buy?
- If buy, do we want this to be a
  - JV/partnership (with, e.g., economic participation), or a
  - Standard vendor engagement?
- Does an *existing* vendor offer this functionality (or will they)? Perform an environmental scan of your existing projects and the market.
- How would the product be incorporated into our workflows. Could it leverage existing systems or workflows? Would it require a new or adjusted workflow?

The answers will guide your strategy and negotiations.

Assess the vendor & conduct due diligence, cont.

- **Ask questions**:
  - If the product utilizes an AI model – “Who developed the model, your company or another company?” And “Does your company own the AI product/functionalities? If not, who does?”
  - Consider the likely impact on your IT infrastructure and FTE work – “Would you seek to integrate the AI product/functionalities into any of the products/workflows we employ? If so, explain how you propose this would work.”
  - Consider vendor incentives (e.g., to get your data), vendor’s privacy-law expertise/whether you trust them with your data – Could ask: “Do you have privacy counsel we can talk to?”
  - Do you seek to use our data to improve your product or train your AI product/model?

Recent Guidance:
Joint Commission and Coalition for Health AI (CHAI)

The Responsible Use of AI in Healthcare (RUAIH)

- “The promise and opportunity of artificial intelligence (AI) tools in healthcare are transformative….The transformative opportunity that AI presents is not without risk, however.”
- Describes seven elements of responsible AI use: (1) AI Policies and Governance Structures; (2) Patient Privacy and Transparency; (3) Data Security and Data Use Protections; (4) Ongoing Quality Monitoring; (5) Voluntary, Blinded Reporting of AI Safety-Related Events; (6) Risk and Bias Assessment; (7) Education and Training