HCRR 114 Managing AI Tools: Oversight, Risk, and Compliance in Practice

Presented May 20, 2026 by PYA's Valerie Rock, Miriam Murray, and Erin Walker | Part of the Healthcare Regulatory Roundup Webinar Series

https://www.pyapc.com/insights/hcrr-114-webinar-managing-ai-tools-oversight-risk-and-compliance-in-practice/

Please note, this transcript was generated automatically. PYA cannot guarantee its accuracy or completeness.

WEBINAR SUMMARY

This episode of PYA's Healthcare Regulatory Roundup webinar series focused on managing AI tools, emphasizing the importance of oversight, risk, and compliance in healthcare. Presenters Valerie Rock, Miriam Murray, and Erin Walker discussed the need for a robust infrastructure to ensure AI's safe and effective use. Key points included the necessity of governance, risk assessments, and vendor due diligence. They highlighted the importance of human oversight, particularly in clinical and operational settings, to mitigate risks such as bias, inaccuracy, and privacy breaches. The discussion also covered the integration of AI into existing compliance structures, the role of frontline teams in monitoring AI outputs, and the importance of clear communication channels for reporting issues.

Key topics and takeaways include:

- AI is widely used in healthcare, often embedded in tools and workflows without formal review or transparency.
- Oversight and governance are critical to manage risks such as bias, inaccuracy, privacy breaches, and audit exposure.
- Organizations must maintain an up-to-date inventory of all AI tools in use, including those from vendors.
- Human oversight is essential—frontline staff must review and validate AI outputs, especially in clinical and operational settings.
- AI oversight should be integrated into existing compliance, quality, and patient safety frameworks.
- Risk assessments for AI should be ongoing and included in enterprise risk management processes.
- Vendor due diligence must go beyond traditional checks to address AI-specific risks, including data use, transparency, and audit rights.
- Clear accountability and defined ownership for each AI tool are necessary.
- Policies and training should address acceptable use, data handling, and reporting of issues or anomalies.
- Reporting channels (e.g., compliance hotline, IT help desk) should be accessible for staff to escalate AI-related concerns.
- Multidisciplinary teams (compliance, IT, clinical, legal) should be involved in AI oversight and decision-making.
- Contracts with AI vendors should include requirements for notification of changes, data ownership, and exit clauses.
- Continuous monitoring, auditing, and revalidation of AI tools are required as models and outputs evolve.

FREQUENTLY ASKED QUESTIONS

What was the main message of this webinar?

- The main message was that AI can support healthcare operations, but organizations need a defensible oversight structure. The presenters emphasized governance, inventories, data safeguards, human review, vendor diligence, monitoring, and reporting processes.

Why do healthcare organizations need an AI inventory?

- An AI inventory helps an organization identify where AI exists, who uses it, what data it touches, which vendor or internal owner is responsible, and what oversight is required. Without an inventory, organizations may not know what they need to govern.

What is shadow AI?

- Shadow AI refers to AI tools or features that individuals or departments use without formal review, approval, governance, or visibility from compliance, privacy, legal, security, or IT teams.

How should AI fit into an existing compliance program?

- AI should be integrated into existing compliance, HIPAA privacy and security, enterprise risk, quality, patient safety, user access, and vendor management processes. The presenters cautioned against treating AI as a separate silo.

What does human-in-the-loop review mean?

- Human-in-the-loop review means a trained person reviews AI inputs or outputs before they are used for documentation, coding, compliance research, clinical decision support, or other operational decisions. The reviewer should have the knowledge needed to validate the output.

Why is human review especially important for clinical documentation and coding?

- AI-generated notes, coding suggestions, and charge capture recommendations may improve efficiency, but inaccurate outputs can create documentation, billing, compliance, and audit risk. The presenters emphasized that the medical record should still reflect the clinician's professional judgment.

Is embedded AI in an EHR only the vendor's responsibility?

- No. The presenters stated that organizations still need internal oversight for embedded AI that influences care decisions, alerts, workflows, documentation, or operations. Vendor involvement does not eliminate the organization's responsibility to understand and monitor use.

What should organizations consider before using AI with PHI or PII?

- Organizations should define minimum necessary data standards, configure tools to match approved data-use limits, train users on what they may input, assess HIPAA privacy and security implications, and understand what happens to data after it enters the tool.

How is AI vendor due diligence different from traditional vendor review?

- AI vendor diligence should go beyond traditional security questionnaires. Organizations should understand intended use, data sources, data ownership, secondary use of data, model updates, bias, drift, transparency, audit rights, security safeguards, and termination options.

What should staff do if an AI tool produces an error or unexpected output?

- Staff should have a clear reporting channel, such as a compliance hotline, IT ticketing system, AI governance email, or escalation process. The organization should document the issue, review it, determine corrective action, and involve the vendor when needed.

How can organizations monitor AI after implementation?

- Organizations can use periodic reviews, risk assessments, data analytics, trend monitoring, user feedback, accuracy checks, bias monitoring, workflow impact reviews, and revalidation after material updates or configuration changes.

ACTION ITEMS

- Establish a formal AI governance structure that clearly designates ownership for each AI tool (clinical, operational, and administrative) and documents use cases, accountability, and decision rights.
- Build and maintain an enterprise-wide AI inventory (including "shadow AI" and embedded features in EHRs and vendor tools) so you can see where AI exists, what data it touches, and who uses it.
- Integrate AI risk into existing enterprise risk, quality, and patient safety assessments, rather than treating AI as a separate silo, so its impact on care, billing, privacy, and operations is evaluated holistically.
- Define and enforce minimum necessary data standards for AI use (especially PHI and PII), configure tools to respect those limits, and train staff on what they may and may not input.
- Require human-in-the-loop review for AI-generated clinical documentation, coding suggestions, and decision support outputs, with clear expectations that clinicians and staff must "trust but verify."
- Incorporate AI explicitly into compliance, HIPAA privacy/security, user access, and vendor management policies, and ensure those policies are easily accessible and understandable to frontline teams.
- Enhance vendor due diligence beyond traditional questionnaires to understand how each AI tool works, what data it uses, how outputs are generated, and how the vendor manages model updates, bias, and drift.
- Embed AI-related clauses in contracts (BAAs and MSAs) that address data ownership, secondary use of data (including de-identified data), transparency, audit rights, security safeguards, and clear out-clauses if risk becomes unacceptable.
- Implement ongoing auditing and monitoring of AI tools (accuracy, bias, error patterns, workflow impact), and revalidate performance whenever there are material updates or configuration changes.
- Stand up simple, well-publicized reporting channels (e.g., compliance hotline, IT ticketing, or AI governance email) for staff to report AI errors, anomalies, or safety concerns, with defined escalation and response processes.
- Use data analytics and trend monitoring (e.g., coding patterns, denials, clinical outcomes, alert behavior) to detect where AI may be amplifying errors, introducing bias, or driving unintended practice changes.
- Provide targeted education and refreshers for clinicians, executives, and IT on AI capabilities and limitations, emphasizing that AI tools are advisory—not the ultimate decision-makers—and reinforcing accountability.
- Ensure that embedded AI in EHRs and other clinical systems is not treated as "the vendor's problem"; assign internal owners, define how alerts and recommendations are used, and measure impact on patient safety and liability.
- Form multidisciplinary AI review teams (clinical, compliance, legal, privacy/security, IT, operations, and revenue integrity) to evaluate new AI tools, oversee existing ones, and align AI use with organizational objectives.
- Regularly revisit AI use cases and value propositions to avoid scaling flawed processes, confirm that tools still deliver benefit, and adjust or sunset tools that no longer meet risk, quality, or financial expectations.

WEBINAR OUTLINE

Introduction and Overview of CMS Proposed Rules Focus

- PYA Moderator introduces the webinar, and the presenters: Valerie Rock, Miriam Murray, and Erin Walker.
- The presenters each explain their specialties and experience, each bringing different perspectives on AI tools.
- Valerie Rock details her revenue integrity and coding compliance and operational experience, and emphasizes the importance of creating an infrastructure for AI to ensure safe and effective use, highlighting the need for due diligence and oversight.
- Erin Walker discusses her background in regulatory compliance and operational HIPAA privacy and security. She notes the increasing use of AI in various compliance programs, emphasizing the need for appropriate onboarding and oversight to ensure privacy, security, and regulatory compliance.
- Miriam Murray outlines her focus on operational and regulatory compliance risks, vendor relationships, and effective human oversight in AI environments.

Operational and Regulatory Risks in AI Adoption

- Miriam Murray highlights the rapid adoption of AI without proper oversight, creating gaps in governance and increasing risks.
- She notes AI adoption is moving faster than governance, leading to constant monitoring and revalidation of AI models and outputs.
- Miriam walks through the risk of using AI without oversight includes privacy risks, biased outputs, unsupported billing decisions, and potential audit issues.
- She explains that AI is embedded in various systems, including EHRs, revenue cycle tools, and vendor solutions, often without formal review or transparency from vendors.
- Miriam emphasizes that appropriate oversight is critical in clinical and operational sections, as well as in compliance, privacy, coding, administrative, human resources, and legal functions to mitigate risk.
- She details highlights potential risk for PHI and PII exposure; validating data quality, potential bias, accuracy, and storage; and third party/vendor AI use.

Foundational Elements of AI Management

- Erin Walker emphasizes the importance of governance, starting with a clear understanding of who owns the AI and what data is being used (e.g., PHI, billing/financial, organizational, etc.).
- She details ways foundational security elements include inventorying all AI tools, ensuring data use and handling comply with regulations, and configuring tools and security alerts appropriately.
- Erin explains that risk assessments should integrate AI into existing risk assessments to ensure comprehensive oversight.
- She notes vendor risk management is particularly critical, and should go beyond traditional due diligence to understand how AI tools work and their impact on data.
- Erin further explains that vendors' internal AI measures and security guarantees cannot be relied upon as the main AI security oversight. Healthcare organizations and providers are ultimately responsible for their own security, auditing, and risk management.
- She describes ways security safeguards and guardrails should treat AI tools similarly to other applications, with appropriate encryption, configuration, multi-factor authentication, and access controls.

- Erin walks through key questions organizations should be able to answer regarding AI algorithms, including: who has ownership of the tool; how over-reliance is prevented; how performance, drift, and bias are monitored and corrected; how adverse/near miss events are investigated and remedied; how alert fatigue is assessed and addressed; and can the organization explain the AI's operation, function, limitations, and role within care pathways.

Integrating Oversight into Compliance Structures

- Miriam Murray discusses regulatory expectations for AI integration and oversight, focusing on the need for clear accountability, defined governance processes, and documented risk assessments.
- She explains AI tools should be integrated into existing policies, including HIPAA privacy and security, compliance programs, and user access.
- Miriam emphasizes that ongoing auditing and monitoring and documentation are essential to ensure AI tools operate as expected and in accordance with quality measures, and so organizations can identify and address any issues promptly.
- She details why transparency and accountability is crucial, with leadership and employees understanding AI tool use and reporting channels for issues.
- Miriam highlights the necessity of training and education to ensure staff understand AI tool limitations and proper use, relevant privacy and bias risks, and human in the loop accountability.

Human in the Loop and Frontline Responsibility

- Valerie Rock emphasizes the importance of the human in the loop approach, where frontline teams review AI outputs for accuracy.
- She stresses that frontline teams must be trained in proper processes for AI tool vetting, business associate agreement requirements, correct usage and accountability monitor AI outputs and report any issues through established channels, such as a hotline or IT help desk.
- Valerie explains the compliance department should have a process to review and address AI-related issues, ensuring comprehensive oversight.
- She notes that best practices include defining and training on AI tool use, implementing expected review processes, and aligning skill sets with oversight responsibilities.
- Valerie highlights ways data analytics can help monitor AI tool usage and identify potential issues, ensuring continuous improvement and compliance.
- She discusses that providers should use AI as a tool and opportunity to develop closer connections and empathy with patients, not to take over clinical decision-making.

Vendor Due Diligence and Contracting

- Valerie outlines the importance of vetting AI vendors for risk areas, including intended use, data use, and output review processes.
- She notes contracts should include expectations for vendor communication of material changes and out clauses for termination if necessary.
- Valerie explains customization of AI tools should be monitored to ensure continued relevance and effectiveness.
- She mentions that leveraging NIST and ISO methods for AI tool monitoring and diligence is recommended for best practices.

- Valerie discusses that ensuring ownership of data and understanding data use agreements are critical to mitigating risks and maintaining compliance.

Conclusion and Resources

- Valerie Rock concludes by emphasizing the importance of functional AI use, creating an infrastructure for oversight, and educating teams on proper AI tool use.
- She encourages participants to ask questions and engage in further discussion on AI tools and compliance.
- PYA Moderator provides contact information for further questions and mentions that slides and recordings of the webinar are available at pyapc.com.