Healthcare Regulatory Roundup #114

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

May 20, 2026

Housekeeping

- Slides, handouts, and forms available in **Resources Panel**
- Enter questions in **Q&A Panel** – questions will be responded to via e-mail after the webinar
- Enlarge, rearrange, or close panels as you prefer
- For technical difficulties, try refreshing your browser

Introductions

Valerie Rock
Principal
vrock@pyapc.com

Miriam Murray
Senior Manager
mmurray@pyapc.com

Erin Walker
Manager
ewalker@pyapc.com

PYA
pyapc.com
865.673.0844

ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

Today's Agenda

1. Common AI-Related Operational and Regulatory Risks
2. Managing AI Tools, Technology, and Vendor Risk
3. Integration of AI Oversight into Compliance Infrastructure
4. Human-in-the-Loop Oversight
5. AI-Specific Vendor Due Diligence

1. Common AI-Related Organizational and Regulatory Risks

AI Is Here to Stay

- Organizations are already using AI – whether or not it is labeled as such
  - AI-enabled vendor tools
  - Embedded AI features in electronic health records (EHRs), human resources platforms, revenue cycle tools, compliance tools, etc.
- In many cases, AI adoption is occurring faster than governance, documentation, and oversight structures can adapt
- Implementation of AI is not just a single, one-time project
- It's not the risk of simply using AI – it is using it ***without appropriate oversight, governance, and continued monitoring***

Common Uses of AI in Healthcare

Clinical and Operations

- Clinical documentation
- AI-assisted coding and charge capture
- Diagnostic support tools embedded in imaging platforms
- Patient triage and symptom checking

Compliance, Privacy, and Legal

- Chatbots answering compliance or human resources questions
- Automated auditing and monitoring and anomaly detection

Administrative

- Resume screening and candidate ranking
- Performance analytics
- Employee surveys

The Risk Reality

Privacy and Security	Potential exposure or misuse of protected health information (PHI) and personally identifiable information (PII) due to inadequate safeguards, logging or data retention practices
Regulatory and Legal	Unclear HIPAA applicability, missing business associate agreements, evolving regulatory expectations, and insufficient compliance documentation
Clinical and Operational Safety	Risk of inaccurate, biased, or non-explainable AI outputs influencing care or business decisions without appropriate human oversight
Data Quality and Bias	AI models may rely on incomplete or biased data, leading to unreliable results or inequitable outcomes
Vendor and Third-Party Risk	Limited transparency into AI vendors' data use and retention, security controls, subcontractors, and model governance
Governance and Oversight	Lack of formal AI governance, usage approvals, policies, training, and accountability processes

2. Managing AI Tools, Technology, and Vendor Risk

Key Areas Organizations Must Manage

- Governance and accountability
  - Formal approval processes and defined oversight bodies (e.g., AI subcommittee, IT governance)
  - Clear assignment of responsibility for risk, privacy, security, and operations
- AI inventory and use case register
  - Maintain an AI inventory and use-case register
  - Document tools, technologies, vendors, intended use, and data interactions
- Data use and handling
  - Apply minimum necessary principles
  - Configure tools to limit data exposure
  - Prohibit PHI/PII in unapproved AI tools and technologies and require documented approvals for exceptions

Key Areas Organizations Must Manage (cont.)

- Risk assessment and change management
  - Incorporate AI into existing risk assessment processes
  - Evaluate data flows, intended use, re-identification risk, and emerging threats
  - Reassess at least annually and when material changes occur
- Third party and vendor risk
  - Expand vendor due diligence to address design, data use, subcontractors, and change management
  - Require transparency, audit rights, security risk assessment, and ongoing compliance reviews
- Security and safeguards
  - Define baseline AI security requirements (e.g., encryption, multi-factor authentication, vulnerability management)
  - Integrate AI tools and technologies into existing security monitoring and controls

Scenario 1 – AI-Generated Clinical Documentation in Patient Care

- **Scenario**
  - A healthcare clinic has deployed an ambient listening tool to generate visit notes and suggested orders.
  - The audio and transcript may contain PHI and be processed by a third-party AI platform.

- **Risks**
  - **PHI exposure**
  - **Secondary use**
    - There must be contractual controls and technical constraints in place
  - **Clinical integrity**
    - If staff over-rely on generated notes/orders without appropriate review (“human-in-the-loop”)

Scenario 1 –
AI Scribe/Transcription in Patient Encounters

The organization should be able to answer the following questions:

1. Was the use of the tool formally approved and included in the AI inventory?
2. Do we have a business associate agreement that specifies required safeguards?
3. Where does the audio/transcript go?
4. Who can access it? Is minimum necessary enforced?
5. Is the recording retained? For how long?
6. Is the recording used to train models?
7. Does the user have the right to delete the recording?
8. What are our audit rights?
9. What is our human review standard before documentation becomes part of the medical record (i.e., how to we audit to ensure the documentation is appropriate/correct)?

Scenario 2 – Predictive Algorithms Embedded in Clinical Workflows

- **Scenario**
  - The EHR includes a predictive tool (i.e., sepsis risk scoring) that influences triage, alerting, or care pathways.

- **Risks**
  - **Patient safety and liability**
    - If performance changes or bias exists, harm can occur when the tool is “just advisory”
  - **Operational**
    - Alert fatigue and workflow disruption if governance is absent
  - **Regulatory**
    - ONC’s HTI-1 final rule expects healthcare organizations to be able to explain, document, and oversee how predictive algorithms in certified EHRs influence clinical decisions

Source: https://healthit.gov/regulations/hti-rules/hti-1-final-rule/

Scenario 2 –
Predictive Algorithm Embedded in EHR (Sepsis Risk/Readmission/Triage)

The organization should be able to answer the following questions:

1. Who owns oversight of the tool and how are approvals, changes, and escalations documented?
2. How is the tool's advisory role defined, communicated, and enforced to prevent over-reliance?
3. How does the organization monitor performance, drift, and bias over time? What is the process for responding to issues as they arise?
4. How are adverse events or near misses linked to the tool identified, investigated, and remediated?
5. How is alert fatigue assessed and managed to avoid disruptions to clinical care?
6. Can the organization explain how the tool works, its limitations and its role in care pathways consistent with ONC HTI-1 expectations?

3. Integration of AI Oversight into Compliance Infrastructure

Regulatory Expectations

- AI oversight is not a standalone oversight program – it is an extension of existing compliance, quality, patient safety, and operational frameworks
  - Organizations are expected to demonstrate documented oversight and decision-making, particularly where AI influences clinical or operational outcomes
  - Where AI influences care decisions, oversight expectations align closely with quality and patient safety standards
- Regulators and enforcement agencies expect AI-related risks to be identified, governed, and addressed using the same infrastructure applied to other high-risk activities
- The focus is not on the technology itself, but how organizations control, monitor, audit, and respond to the risk created by its use both initially and over time

What Regulators Expect to See

- Clear Accountability
- Documented Intended Use
- Integrated Policies and Controls
- Ongoing Auditing and Monitoring
- Transparency
- Training and Awareness
- Issue Reporting and Response

Integrating AI Oversight into Existing Operations

- Assign clear accountability
  - Who is responsible for reviewing, approving, and escalating AI-assisted tool decisions?
- Document intended use
  - How are AI tools expected to be used and how are they not to be used? Does the use align with clinical, billing, quality, compliance, and operational objectives?
- Policies and controls
  - Are AI use expectations incorporated into existing compliance, privacy, and security policies?
  - Are there approval, access, and monitoring controls for use of the AI tools?
- Ongoing auditing and monitoring
  - Are AI tools and technologies included in risk assessments, internal audits, and quality reviews?
  - Is reliance on AI outputs monitored to identify trends or anomalies?

Integrating AI Oversight into Existing Operations (cont.)

- Transparency
  - Do leadership and oversight bodies understand where and how AI is used?
  - Is documentation supporting decision-making and oversight maintained?
- Training and awareness
  - Are staff trained on appropriate AI use and limitations?
  - Does the organization reinforce that professional judgment and accountability remain with humans, not the AI tool/technology?
- Issue reporting and response
  - Is there a documented process for incident reporting and escalation of AI-related concerns?
  - When issues arise, are decisions, overrides, and corrective actions documented?

4. Human-in-the-Loop Oversight

Human in the Loop Oversight

Human in the Loop oversight is critical

- Patient care, billing, and compliance decisions carry regulatory risk
- AI outputs can be incomplete or biased
- Over-reliance on AI undermines professional judgment
- Accountability cannot be delegated to a tool or vendor

AI risk is enterprise risk

- Operational
- Clinical/Quality
- Financial
- Regulatory
- Reputational

Common Gaps in AI Oversight

- AI tools are implemented faster than governance structures can adapt, often bypassing existing compliance or IT review processes
- Ownership of AI-assisted decisions is unclear or not formally assigned across compliance, operations, and clinical teams
- AI outputs are incorporated into workflows without consistent validation, monitoring, or defined review expectations
- Documentation does not clearly support how AI tools are approved, used, or overseen over time
- Staff rely on AI-generated outputs without fully understanding limitations, risks, or accountability expectations
- Escalation pathways for inaccurate, biased, or unexpected AI outputs are undefined or inconstantly followed

What This Looks Like in Practice – Effective Human in the Loop Oversight

AI use cases are routed through existing governance structures, with clear ownership for approval, oversight, and escalation

Expectations for how AI tools can and cannot be used are defined at implementation and reinforced through policies and workflows

Human review requirements are aligned to the risk and impact of the AI use case, especially when influencing clinical, financial, or compliance decisions

AI-assisted decisions are subject to ongoing monitoring, including periodic review for accuracy, bias, and over-reliance

When issues arise, organizations can trace how AI outputs were used, escalated, and resolved through documented processes

Training emphasizes critical evaluation of AI outputs and reinforces that accountability remains with the individual—not the tool

5. AI-Specific Vendor Due Diligence

Why AI Vendor Due Diligence and Oversight Matters

- Traditional vendor risk management wasn't designed for tools and technologies that generate conclusions, recommendations, or decisions.
  - AI requires deeper, ongoing diligence – not just intake questionnaires
    - AI vendors can influence clinical, financial, and compliance decisions
    - Over-reliance on vendor assurances creates accountability gaps
    - AI models, data sources, and outputs may change over time
  - Effective oversight of AI vendors
    - Integrated into existing vendor management and procurement processes
    - Risk-based, aligned to the AI use case and impact
    - Clear understanding of vendor responsibilities vs. organizational accountability
    - Ongoing monitoring and reassessment
    - Coordinated across compliance, privacy, security, and operations

AI Vendor Due Diligence Checklist

1. Governance and intended use

- ☐ What problem is the AI tool/technology intended to solve and how will outputs be used?
- ☐ Who is responsible for reviewing and approving AI-generated outputs?
- ☐ Can outputs be overridden, and by whom?

2. Data use and privacy

- ☐ What data does the AI tool/technology access, ingest, or retain?
- ☐ Is PHI, PII or other sensitive data used or stored?
- ☐ How is data minimized, segregated, and protected?
- ☐ If de-identified data is used, what is the criteria for de-identification?

3. Model transparency and limitations

- ☐ What data sources and assumptions influence the AI's outputs?
- ☐ How does the vendor address bias, accuracy, and known limitations?
- ☐ How are model updates and changes communicated?

4. Human in the Loop controls

- ☐ Where is human review required before action is taken?
- ☐ What safeguards exist to prevent over-reliance on AI outputs?
- ☐ How are incorrect or questionable outputs handled?

AI Vendor Due Diligence Checklist (cont.)

5. Monitoring, escalation, and auditability

- ☐ How are issues, errors, or anomalies reported and resolved?
- ☐ Can decisions influenced by AI be audited and reconstructed?
- ☐ What documentation is available to support oversight and accountability?

6. Vendor accountability

- ☐ What contractual terms address transparency, cooperation, and audit rights?
- ☐ How does the vendor support regulatory inquiries or investigations?
- ☐ What happens if the tool no longer meets compliance expectations?

Our Next Webinars

Tuesday & Wednesday, June 23 & 24; 11 am – 1:30 pm ET

PYA's 5th Annual Summer CPE Symposium
Hot Topics in Healthcare & Accounting

4 Sessions, 2 Days, 4 CPE credits available

Please leave a comment regarding topics for future HCRR webinars!

Thank you for attending!

PYA's subject matter experts untangle the latest industry developments every month in our popular Healthcare Regulatory Roundup webinar series.

For on-demand recordings of this and all previous HCRR webinars, and information on upcoming topics and dates, please follow the link below.

pyapc.com/hcrr-webinars

pyapc.com | 865.673.0844

ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

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