Do You Know Where AI Is Putting Your Practice at Risk?

A First Step for Urgent Care and Occ Med Leadership

AI is already showing up in many urgent care and occupational medicine groups, whether leadership planned for it or not. It may be obvious in ambient scribing, intake tools, or coding support. It may also be quieter, hiding inside vendor-added features or casual staff use of public AI tools.

This checklist is a practical first step to help leadership see where that risk may already exist, slow down the wrong decisions, and treat AI as part of a broader cybersecurity, privacy, and operational risk conversation before convenience turns into avoidable exposure.

1. Assume AI Is Already in Your Environment

Do not assume AI only matters when you buy a new AI vendor. AI may already be present in:

- ambient scribing or documentation tools
- call, chat, intake, or scheduling tools
- coding and billing tools
- EHR, PM, RCM, CRM, or communication platforms with added AI features
- staff use of public AI tools for work

Start by identifying what is already in use, what features were added quietly, and what tools touch patient data, employer-related data, billing data, or sensitive internal information.

2. Define the Use Case Before You Approve It

Before approving a tool or workflow, ask:

- What problem are we trying to solve?
- Does this use case actually need AI?
- How much risk does it create?

A simple way to think about risk:

- **Lower impact**: easier to detect and correct; does not materially affect care, major financial outcomes, or sensitive data handling
- **Moderate impact**: supports work that humans still review closely and control directly
- **Higher impact**: materially influences documentation, coding, billing, patient communication, employer communication, or routing decisions
- **Critical impact**: could substantially influence patient safety, major financial outcomes, or highly sensitive operational decisions

3. Focus First on the Highest-Risk Use Cases

For most small urgent care and Occ Med groups, the first areas that deserve closer review are:

- **ambient scribing**
- **call and chat intake**
- **coding and billing assistance**
- **staff use of public or general-purpose AI tools**
- **AI features embedded in existing vendor platforms**

These are the areas where convenience can quickly turn into privacy, workflow, billing, or accountability problems.

4. Put Basic Staff Guardrails in Place

Smaller groups don't need a hospital-scale program to begin. They need clear baseline rules.

At minimum, leadership should decide:

- which AI tools are approved for work use
- which tools or uses are prohibited
- which uses require leadership, compliance, IT, security, or clinical review first
- how staff should report inaccurate, risky, biased, or surprising outputs

Make clear that free or personal AI tools should not be used casually for patient-facing, employer-facing, or sensitive internal work.

5. Review the Vendor, Not Just the Demo

For higher-risk tools, ask:

- What does the AI actually do in the workflow?
- What data does it use, store, or transmit?
- Is a BAA available where appropriate?
- Can customer data be used for model training or broader product improvement?
- What outside models, APIs, cloud providers, or subprocessors are involved?
- How are outputs reviewed, corrected, or overridden?
- How are updates communicated?
- What happens if the output is wrong or degrades over time?

6. Treat the Contract, Rollout, and Monitoring as Part of the Decision

For higher-risk tools, leadership should understand:

- what the vendor can and cannot do with practice data
- what notice is required before meaningful updates or changes
- what obligations the vendor has if there is a security issue or major performance problem
- how the tool will be tested before broader use
- what the human review step is
- what happens if the tool becomes unreliable, changes unexpectedly, or goes away
- how data will be returned or destroyed if the relationship ends

Approval should not be the end of the process. Recheck performance after rollout. Reassess after major updates. Revisit the tool at renewal, not just at purchase.

7. Add Urgent Care and Occ Med-Specific Caution Where It Matters

For urgent care, pay close attention to tools that affect intake, patient routing, documentation, and billing.

For occupational medicine, be especially careful with anything that affects employer-facing summaries, work status communication, return-to-work language, or reporting that sits close to both clinical and employment-related concerns.

For hybrid groups, assume a tool purchased for one workflow can create consequences elsewhere.

Red Flags That Should Slow You Down

These do not automatically end the conversation, but they should change the tone of the conversation.

- “You do not need to worry about review because the system is highly accurate.”
- “We cannot provide meaningful documentation because the system is proprietary.”
- “We use customer data to improve the platform in general.”
- “This feature was added automatically as part of the platform.”
- “Your team can use their own judgment on whether public AI tools are fine.”
- “It is just an administrative feature, so privacy and workflow review are not really necessary.”
- “We update the feature regularly, but there is no need to notify you unless something major happens.”

Final Leadership Questions

- Do we know where AI is already in use across our practice?
- Have we defined the use case before approving the tool?
- Are we treating higher-impact workflows differently from lower-impact ones?
- Do we have a documented human review step where the workflow calls for it?
- Do we understand what the vendor can do with our data?
- Do we know what happens if the tool becomes unreliable, changes unexpectedly, or goes away?

This is a practical first step, not a complete AI governance program.

This checklist was prepared by Ira Pasternack and informed by the *Third-Party AI Risk and Supply Chain Transparency Guide* from the Health Sector Coordinating Council Cybersecurity Working Group.

https://healthsectorcouncil.org/ai-cyber-thirdparty/