

AI in Healthcare: Compliance & Safety Checklist for Practices

Security & Privacy

- ☐ **Include AI tool or AI-enabled devices in your Security Risk Analysis (SRA)**
 - Evaluate how AI tool or AI-enabled devices interact with PHI
 - Identify risks like data storage, access, and third-party exposure
 - ☐ **Confirm if the AI tool or AI-enabled device is HIPAA compliant**
 - Check whether it stores or transmits PHI
 - Verify if it offers HIPAA-compliant settings (e.g., enterprise versions)
 - ☐ **Use platforms with proper data safeguards**
 - Ensure data is encrypted at rest and in transit
 - Use secure access controls and audit logs
 - ☐ **Maintain a current Business Associate Agreement (BAA)**
 - Required for any vendor or tool handling PHI on your behalf
-

Vetting & Monitoring AI Tools

- ☐ **Confirm the AI's intended use fits your clinical setting**
 - Avoid using general-purpose AI for diagnostic or clinical decision-making without human oversight
 - ☐ **Evaluate the tool's accuracy and reliability**
 - Regularly review outputs for errors, hallucinations, or outdated information
 - ☐ **Audit and monitor usage regularly**
 - Track how tools are used
 - Monitor for inappropriate prompts or data input
-

AI in Healthcare: Compliance & Safety Checklist for Practices

Staff Training & Awareness

- ☐ **Train staff on appropriate AI use**
 - What AI can/can't do
 - When not to enter PHI
 - Risks of overreliance or misuse
 - ☐ **Ensure staff understands patient privacy rules**
 - Never input identifying details into unapproved AI tool or AI-enabled devices
 - Be cautious with tools that auto-sync with EHR or messaging platforms
 - ☐ **Provide refresher training at least annually**
 - Include examples and policy updates related to AI
-

Policy & Documentation

- ☐ **Update internal policies and procedures to address AI**
 - Define approved tools and use cases
 - Specify who is allowed to use AI
 - Outline required safeguards
 - ☐ **Include AI guidance in the employee handbook**
 - Cover dos and don'ts
 - Reinforce consequences of policy violations
 - ☐ **Keep documentation of risk assessments and compliance steps**
 - For internal use and potential audits
-

AI in Healthcare: Compliance & Safety Checklist for Practices

Ongoing Review & Updates

- ☐ **Reassess AI tool or AI-enabled devices regularly**
 - Especially after major updates or new feature releases
 - ☐ **Watch for changes in HIPAA, FTC, and state privacy laws**
 - AI regulations are evolving—stay informed
 - ☐ **Engage compliance or legal counsel if unsure**
 - Especially before rolling out new AI tool or AI-enabled devices or integrations
-

Optional Practice Tips

- ☐ Create a centralized log of AI tool or AI-enabled devices in use
- ☐ Appoint an **AI compliance lead** or include it in your Privacy Officer's responsibilities
- ☐ Test AI tool or AI-enabled devices in a sandbox environment before full implementation