AI Trust & Security Checklist

A guideline for healthcare & education leaders reviewing AI tools and the companies that provide them.

1. Trust & Transparency

- ☑ **About Us Page –** Confirm the tool you're using comes from a company with a clear mission, values, and contact info.
- ☑ **Transparency –** Look for clear, accessible policies on data usage, compliance, and risks. Consider vague or hidden details a red flag.
- ☑ **Community Proof –** Review published case studies, testimonials, or partnerships with universities/hospitals.

2. Security & Compliance

- ☑ **Security Policy –** Check for encryption, access controls, and data handling practices. Ask whether tools let you opt out of training their models.
- ☑ **Legal Compliance –** Verify the company has published policies or terms of service and look for explicit mention of standards like FERPA, GDPR, HIPAA, COFEPRIS.
- ☑ **Certifications –** Look for SOC 2, ISO 27001, or similar independent audits.
- ☑ **Incident Response Policy –** Require a clear incident response plan for breaches, misuse, or AI errors, with escalation pathways.

3. Data Stewardship

- ☑ **Data Location & Access –** Validate where your data is stored (U.S., abroad, cloud) and that you can export/download it without vendor delays.
- ☑ **Model Training Controls –** Confirm your data isn't automatically used to train public AI models; safe vendors let you disable this.
- ☑ **Free ≠ Safe –** Carve out a budget for AI tools. Free tools may monetize your data. Paid services are usually more transparent about responsibilities and are more likely to let you opt out of training the algorithms with your data.

4. Effectiveness & Fairness

- ☑ **Clinical/Educational Accuracy & Validation –** Ensure the tool is validated against domain standards (e.g., ACGME, LCME, AACN, AVMA, etc.).
- ☑ **Bias & Fairness –** Review vendor's bias testing across demographics; ensure ongoing monitoring for fairness.
- ☑ **Auditability & Explainability –** Require audit logs of AI use and, where possible, explanations for outputs.

5. Governance & Sustainability

- ☑ **Data Submission Guidelines –** Set policies for employees about the data that can and cannot be entered into AI tools to avoid accidental exposure of sensitive or regulated information.
- ☑ **Role-Based Access –** Establish access controls for who in your institution can use advanced AI features.
- ☑ **Human-in-the-Loop –** Document a review process for critical decisions. AI should assist, not replace, expert judgment.
- ☑ **Lifecycle & Vendor Sustainability –** Assess update policies (model retraining, patches) and vendor stability.
- ☑ **End-User Training & Guidelines –** Ensure vendors provide usage guidelines and training for responsible use.
- ☑ **Ethical & Responsible Use –** Confirm the vendor publishes an ethics statement and defines limits on use cases (e.g., not for direct patient diagnosis, etc.).