Privacy Checklist

- ☐ HIPAA and FERPA compliance explicitly stated
- ☐ Verify existence of Business Associate Agreement (BAA) if third-party vendor involved
- ☐ Data must be encrypted at rest and in transit
- ☐ Verify physical and digital security of server location, access, and monitoring
- ☐ Clear policies for data storage duration, deletion, and backup
- ☐ Ability to restrict access to authorized clinicians only
- ☐ Ability to track changes to client data
- ☐ Tool can function with minimally necessary data and without PHI
- ☐ If data is reused for AI training, confirm in writing that it is de-identified and cannot be re-linked to clients
- ☐ Obtain informed consent for any recording, upload, or use of client data outside direct care
- ☐ Clients must be able to decline use of AI tools without impacts to therapy services
- ☐ Obtain informed consent from parents before use, including:
  - What data is collected, how it used and stored, who has access, and third-party sharing policies

Evaluating Vendors and Tools

- ☐ Confirm privacy statements explicitly state data handling practices, HIPAA compliance, and third-party sharing rules
- ☐ Look for independent security audits, SOC 2, ISO 27001, or other certifications
- ☐ Locate clear policies for vendor to notify users and remediate data breaches as they may occur
- ☐ Ensure tools do not replace clinician judgment
- ☐ Regularly re-assess tools for compliance, updates, and new risks
- ☐ Maintain internal records of tool approval, consents, and security verifications