The HIPAA-Secure Session Note Checklist

A Compliance-Minded Workflow for Mental Health Professionals
Objective: To organize session notes efficiently without introducing unnecessary cloud exposure or third-party risk.

The Checklist

Step 1: Define the Data Scope
Before the session begins:

[ ] Clarify Intent: Determine if this session requires verbatim transcription or just a structured summary.

[ ] Limit Access: Confirm that only the primary clinician has access to the recording device.

[ ] No "Live" Sharing: Ensure no real-time collaboration features are active during the session.

Step 2: Secure the Session Environment
During the session:

[ ] No "Bot" Participants: Verify that no AI scribe bots or third-party attendees have joined the video call.

[ ] Local Recording Only: Use system-level audio capture (on your device) rather than cloud-based recording tools.

[ ] Visible Transparency: If recording, ensure the patient is informed and no "hidden" listeners are present.

Step 3: Verify On-Device Processing
Handling the data:

[ ] Disconnect Test: Can your transcription tool work offline? (If yes, it’s truly local).

[ ] No Cloud Uploads: Ensure audio files are processed strictly on your computer’s hard drive/processor.

[ ] Local AI Generation: Verify that summaries are generated by a local model (e.g., Apple Silicon), not an API call.

Step 4: Separate Device Roles
Managing hardware:

[ ] Primary Device (Mac/PC): Use this for full transcription, processing, and deep storage.

[ ] Capture Device (iPhone/Tablet): Use only for temporary recording or quick recall; do not store long-term data here.

[ ] Clear Cache: Regularly clear temporary recordings from secondary devices after transfer.

Step 5: Safe Storage & Export
Finalizing the note:

[ ] Local Drafting: Edit and finalize clinical notes in a local text editor or the app itself.

[ ] Manual Export: Copy/paste the final note directly into your EHR (Electronic Health Record).

[ ] Disable Auto-Sync: Ensure the folder containing raw transcripts is excluded from iCloud/Google Drive auto-backups.

Why this matters:
Protecting patient data isn't just about software features; it's about architecture. By keeping data local, you reduce the surface area for breaches and maintain stricter confidentiality.
Brought to you by Geode Strictly on-device transcription for professionals.
www.geodeclarity.com