

# The AI Scribe Buyer's Checklist

A printable worksheet for clinicians and practice managers evaluating AI medical scribes. Tick items as you confirm them with a vendor. Curated by a practicing psychiatrist. Sourced facts only - not legal or compliance advice.

## Before you share any patient data

- ☐ **BAA:** will the vendor sign a Business Associate Agreement before any patient data is used?
- ☐ **Data retention:** how long are audio and transcripts kept, and can you set or shorten that?
- ☐ **Model training:** is your data used to train or improve models, and can you opt out in writing?
- ☐ **EHR integration:** direct push into your EHR, or copy and paste?
- ☐ **Consent for recording:** does the tool support capturing and documenting patient consent?
- ☐ **Specialty templates:** are there templates for your specialty (for example psychiatry or therapy notes)?
- ☐ **Pricing model:** price per note or encounter vs flat per month, and any note caps?
- ☐ **Cancellation terms:** monthly vs annual, notice period, and data return or deletion when you leave?

### How to use the official-source pages that follow

Page 2 turns four high-stakes rules into plain language for practices choosing an AI scribe. Each point has a bold rule, what it means in clinic workflow, and a named official source with a link. Read those sources yourself before you sign anything. This worksheet is not a substitute for counsel or your compliance lead.

## Official source points: HIPAA, BAAs, and recording consent

Rules behind the checklist ticks above. Wording tracks HHS guidance and California Penal Code section 632. Confirm with your counsel or compliance lead.

### **Rule: Treat an AI scribe that creates, receives, maintains, or transmits PHI for your practice as a business associate.**

HHS says a business associate is a person or organization (other than a workforce member) that performs certain functions or services for a covered entity involving the use or disclosure of PHI. HHS examples include an independent medical transcriptionist, or the vendor of an app that provides transcription services to a physician, and cloud service providers engaged to process or store ePHI.

For a practice choosing an AI scribe, that usually means you should expect a BAA before any visit audio, transcript, or note content leaves your control - and you should ask which subcontractors also touch that data.

Source: [HHS, Business Associates guidance](#)

### **Rule: Put a written Business Associate Agreement in place before the vendor handles PHI, and make sure it covers the required terms.**

HHS says a covered entity may disclose PHI to a business associate if it obtains satisfactory assurances in a BAA that the associate will safeguard the information. Among other requirements, a BAA must describe permitted and required uses and disclosures of PHI; bar other uses except as permitted by the BAA or required by law; require appropriate safeguards (including Security Rule protections for ePHI); require reporting of unauthorized uses or disclosures and breaches of unsecured PHI; require subcontractors to agree to the same restrictions; and, at termination, require return or destruction of PHI where feasible.

For a practice, ask for the vendor's standard BAA early - including on free tiers and trials - and confirm it addresses subcontractors, breach reporting, and what happens to audio and notes when you cancel.

Source: [HHS, Sample Business Associate Agreement Provisions](#) (see also [HHS, Business Associates guidance](#))

### **Rule: Do not store or process ePHI in a cloud or AI scribe service without a HIPAA-compliant BAA - encryption alone does not remove that duty.**

HHS guidance on HIPAA and cloud computing says that when a covered entity engages a cloud service provider to create, receive, maintain, or transmit ePHI, the provider is a business associate - even if it processes or stores only encrypted ePHI and lacks an encryption key. Using such a service to maintain ePHI without a BAA violates the HIPAA Rules. HHS also states that OCR does not endorse, certify, or recommend specific technology or products.

For a practice, treat marketing claims like "HIPAA certified" as non-official. Ask whether a BAA is available before any real patient data is uploaded, and review how audio and notes are stored.

Source: [HHS, Guidance on HIPAA & Cloud Computing](#)

### **Rule: Recording consent is mostly governed by state law, separate from HIPAA - and some states require consent from all parties to a confidential communication.**

California Penal Code section 632 makes it unlawful to intentionally use an electronic amplifying or recording device to eavesdrop upon or record a confidential communication without the consent of all parties. A "confidential communication" is one carried on in circumstances that may reasonably indicate any party desires it to be confined to the parties (and excludes settings where the parties may reasonably expect it may be overheard or recorded).

Clinical visits often look like confidential communications under that definition. Laws differ by state, so check the rules where you and the patient are located. A cautious practice approach is to ask every patient, document consent, and confirm the scribe tool supports that workflow.

Sources: [California Penal Code section 632](#); [Justia, 50-state recording law survey](#)

## Questions to ask on a vendor demo

Tick each question as you ask it. Bring this page to the call.

- ☐ 1. Can I see your standard BAA, and who are your subcontractors that touch patient data?
- ☐ 2. Where is audio and note data stored, and for how long by default?
- ☐ 3. Is any of my data used for model training? Is that off by default?
- ☐ 4. Show me a full note for a visit in my specialty, start to finish.
- ☐ 5. How do clinicians review and correct a note before it reaches the chart?
- ☐ 6. How does the note get into my EHR, and what happens if the integration fails?
- ☐ 7. What happens to my data if I cancel, and how do I get a copy?
- ☐ 8. What is the all-in price per clinician, including setup, caps, and overage?
- ☐ 9. Can I run a trial with real workflows, and what is the trial length?
- ☐ 10. What security reports (for example SOC 2) can you share under NDA?

## Notes from this demo

Vendor · Date · Who attended · Decision

---

---

---

---

### Get the weekly digest

New tools, price changes, and practical comparisons - free at [clinicalaiweekly.com](https://clinicalaiweekly.com)

[clinicalaiweekly.com](https://clinicalaiweekly.com)

**Disclaimer:** Content is for general information only and is not medical, legal, or compliance advice. Confirm HIPAA terms and sign a Business Associate Agreement directly with any vendor before use. This checklist contains no patient information. ClinicalAIWeekly is curated by a practicing psychiatrist. Listings and sponsorships (if any) never change the wording of this checklist.