

Questions to ask any AI scribe, and our answers.

Adopting an ambient scribe usually means satisfying whoever owns security and compliance. Here's the due-diligence checklist to put to **any** vendor, with Eluve's answers alongside. Ask the same of everyone you evaluate.

Ask every vendor	Eluve's answer
Do you sign a BAA?	Yes. A Business Associate Agreement is available for every practice, executed before any PHI is processed.
Is audio recorded and stored?	Audio is recorded to generate the note; retention is governed by the BAA and our Privacy Policy, contact us for specifics and configuration.
Do you train AI models on our data?	Not on identifiable PHI. Where a practice agrees, de-identified data may be used to improve and train our models, as permitted under the BAA and described in our Privacy Policy and Terms.
What encryption is used?	Data is encrypted in transit and at rest.
Which certifications do you hold?	SOC 2 Type I & Type II; HIPAA and PIPEDA compliant; pursuing HITRUST. SOC 2 report available under NDA.
How is access controlled?	Role-based access control with least-privilege, SSO/SAML support, and audit logs for every action and artifact.
Where is data hosted?	Cloud or your VPC, with regional data residency available. Confirm specifics for your deployment.
Is there tenant isolation?	Yes. No cross-customer data mixing.
How does it integrate with our EHR?	Via HL7v2, FHIR, and REST; the clinician reviews and approves every note before it reaches the record.
Who is accountable for the output?	The clinician. Eluve provides full provenance and audit trails; it supports but never replaces clinical judgment.

The BAA, in plain language.

A Business Associate Agreement is the single most important document when a tool touches PHI. Here's what it is and what to look for: a briefing for clinicians, not a replacement for the agreement itself.

What a BAA is	A contract required under HIPAA between a covered entity (your practice) and a business associate (a vendor that handles PHI on your behalf). It's the floor for compliance; certifications build on top of it.
What it commits the vendor to	Safeguarding PHI, using it only for the agreed services, restricting disclosures, reporting breaches, supporting your patients' rights, and returning or destroying PHI at contract end.
Why it matters for AI scribes	It's what makes it lawful for the tool to process the encounter. A homepage that merely says "HIPAA compliant" is not a substitute for an executed BAA.
What to check	That the BAA is signed before go-live, names subprocessors or references a current list, and states data-retention and breach-notification terms in writing.

Bottom line. The BAA is the floor; SOC 2 Type II, encryption, access controls, and no-training-on-data are what a mature vendor adds on top. Eluve provides all of the above. Request the executed BAA and current SOC 2 report to complete your file.

 Don't forget consent

HIPAA governs how PHI is handled; it does not, by itself, cover **recording** consent. State law and professional ethics govern whether you must inform and get agreement before recording an encounter, and some states require all-party consent. Pair your BAA review with the Eluve consent form, signage, and State Consent Lookup.