# Até que ponto seu anotador com IA é privado?

Anotadores com IA transformam sua reunião em um registro nas mãos de outra pessoa. Saiba o que sai do dispositivo em cada etapa, como verificar as alegações de uma ferramenta e como manter tudo local.

Publicado por Julian Pscheid · 15 de julho de 2026 · Atualizado 20 de agosto de 2026
Ler este artigo online: https://www.hedy.ai/pt/post/how-to-use-ai-meeting-notes-privately/

Dois colegas conversando em uma pequena mesa em um escritório privado com a porta fechada, um iPhone virado para baixo entre eles ao lado de um caderno e uma caneca de café em forma do pato do Oregon Ducks

Resposta rápida Um anotador de reuniões com IA faz três coisas que podem vazar dados de forma independente: transcreve seu áudio, analisa a transcrição e armazena o resultado. A maioria das ferramentas executa as três nos próprios servidores, então a reunião se transforma em um registro pesquisável nas mãos de outra pessoa. Algumas conseguem executar as três em equipamentos que pertencem a você, a única configuração em que nada sobre a reunião sai da sala. Hedy transcreve no dispositivo por padrão em todas as plataformas em que está disponível e, na maioria dos dispositivos atuais, também pode executar a análise no dispositivo. Com o Cloud Sync do Hedy também desativado, nada da conversa chega aos nossos servidores, a menos que você compartilhe explicitamente essa sessão.

A Associated Press publicou este mês uma matéria sobre anotadores com IA no trabalho que cataloga bem os riscos ( AP, julho de 2026 (https://apnews.com/article/ai-notetaker-work-meetings-privacy-data-c700299371ca7cfec77dafdfb948067f) ): informações confidenciais sobre funcionários, estratégia corporativa, segredos comerciais, comentários que mais tarde ficam comprometedores em um

depoimento. Os conselhos também são sensatos. Verifique se um anotador entrou na reunião. Peça consentimento antes de uma reunião delicada. Apoie-se na política da empresa para que nenhuma pessoa precise ser a única a se opor. Desative a ferramenta durante a parte delicada. Pergunte o que o fornecedor retém e se usa algum desses dados para treinamento.

Cada uma dessas medidas administra as consequências de sua reunião se tornar um registro nas mãos de outra pessoa. Nenhuma delas pergunta se isso precisa acontecer. Justin Daniels, advogado corporativo da Baker Donelson, deu à matéria sua frase mais incisiva: "Não começo a falar sobre nada substancial até que a ferramenta seja desligada, porque simplesmente não quero correr esse risco." Esse é o conselho certo para as ferramentas que a maioria das pessoas tem, e parte do pressuposto de que a reunião precisa sair do seu hardware.

Nos dispositivos atuais, a reunião não precisa sair. Um pequeno número de produtos consegue executar todo o pipeline na sua própria máquina, e quase ninguém sabe disso.

## O que sai do dispositivo quando você usa um anotador?

Três coisas, e elas vazam de forma independente. A transcrição transforma seu áudio em texto. A análise lê esse texto e escreve seu resumo e seus itens de ação. O armazenamento determina se alguma parte permanece em um lugar que você não controla. Cada etapa pode ficar em equipamentos que pertencem a você ou passar para os equipamentos de outra pessoa, o que cria oito combinações possíveis.

| Etapa | O que faz | Pode rodar no dispositivo? | O que sai se não rodar |
|---|---|---|---|
| Transcrição | Transforma áudio em texto, às vezes com rótulos de falantes | Sim, em hardware atual | O próprio áudio, além de um embedding acústico por falante em muitos sistemas |
| Análise | Lê a transcrição, escreve resumos e itens de ação | Sim, em hardware capaz | A transcrição e tudo o que um modelo inferir dela |
| Armazenamento e sincronização | Mantém o arquivo | Sim, se permanecer desativado | Uma cópia durável e pesquisável, além de metadados que podem sobreviver à exclusão |

É aí que a maioria das alegações de privacidade se esconde. "O áudio nunca sai do seu dispositivo" soa como uma afirmação sobre o produto inteiro. Significa apenas que a transcrição é local, o que não impede que a transcrição integral, palavra por palavra, seja enviada a um modelo de linguagem um segundo depois. Hedy faz exatamente isso por padrão, e por isso "o áudio sai?" é a pergunta errada para encerrar a investigação. A transcrição é o registro. Quando ela sai da sua máquina, quase tudo com que você se preocupava também saiu.

O processamento híbrido é comum, inclusive no padrão do Hedy. O problema é um fornecedor que não diz quais etapas saem do seu dispositivo.

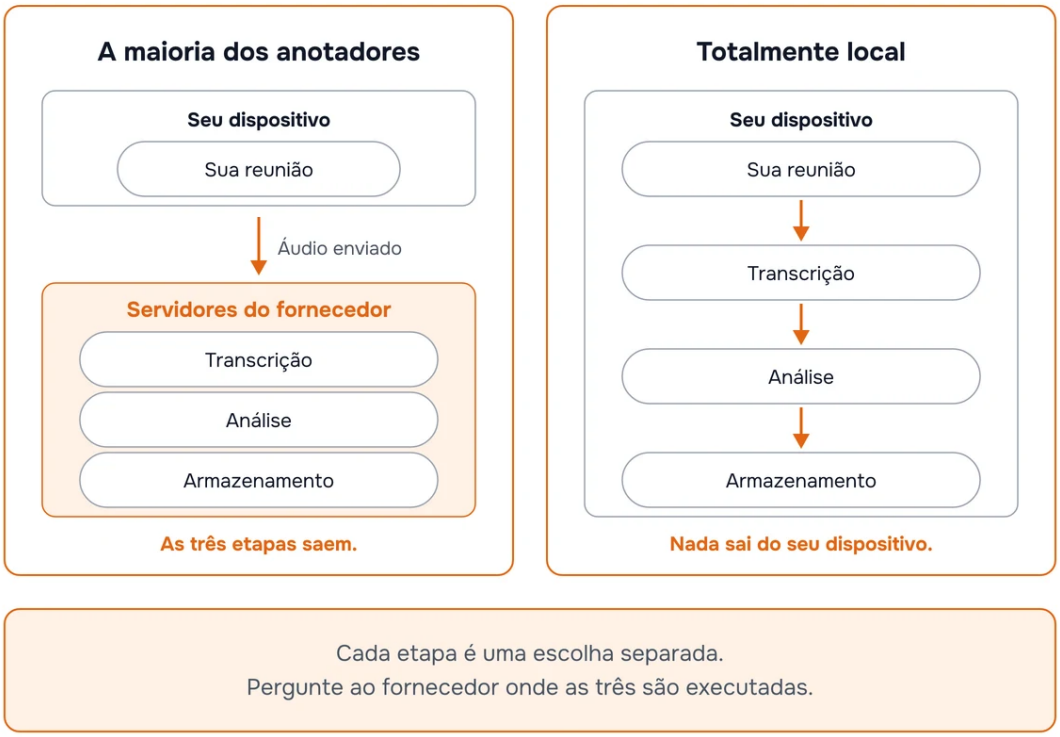


Diagrama comparando a maioria dos anotadores, em que o áudio é enviado aos servidores do fornecedor e a transcrição, a análise e o armazenamento acontecem lá, com uma configuração totalmente local, em que as três etapas acontecem no seu próprio dispositivo

# Todo o pipeline pode rodar no seu dispositivo?

Sim, em hardware atual, e essa é a parte que mudou sem chamar muita atenção. Pouquíssimos produtos executam as três etapas.

## A transcrição é a etapa mais fácil

Whisper, o mecanismo padrão, roda em todas as plataformas em que a Hedy está disponível. O Nemotron roda em todas as plataformas nativas, mas não no app web. O Nemotron é um mecanismo de streaming baseado no modelo de fala de 600 milhões de parâmetros da NVIDIA (https://huggingface.co/nvidia/nemotron-3.5-asr-streaming-0.6b) , e adiciona os rótulos de falantes que antes levavam as pessoas a escolher um mecanismo na nuvem. Ele exige um único download de aproximadamente 0,6 a 0,7 GB e hardware a partir da geração do iPhone 12. A precisão ainda varia com sotaque, ruído ambiente, falas simultâneas e vocabulário especializado, portanto teste-o nas suas próprias reuniões em vez de confiar em qualquer número publicado.

## A análise é onde está a contrapartida

O Processamento de IA Local (/pt/help/local-ai-processing/) executa o resumo e as sugestões na sua máquina e exige hardware de verdade: um Mac com Apple Silicon, um PC Windows com uma GPU capaz ou um iPhone ou iPad recente. Os modelos vão de cerca de 1,2 GB para a categoria móvel a mais de 20 GB. Um modelo intermediário de aproximadamente 9 bilhões de parâmetros roda confortavelmente em um Mac com 16 GB. Os maiores precisam de aproximadamente 25 GB ou mais de RAM.

O Processamento de IA Local vem desativado por padrão porque a análise na nuvem é mais rápida e, atualmente, produz resultados melhores. O padrão do Hedy é uma divisão deliberada: reconhecimento de fala local em todas as plataformas, para que o áudio nunca saia sem que você peça, e análise na nuvem, para que o produto funcione bem em hardware que não consegue hospedar um modelo de linguagem. Um resumo que parece instantâneo na nuvem pode levar de trinta segundos a vários minutos localmente. O artigo técnico aprofundado (/pt/post/local-ai-engineering-deep-dive-hedy-3-2/) apresenta todos os detalhes.

O Processamento de IA Local não faz fallback silencioso para a nuvem. Se algo falhar localmente, você recebe um erro, não uma nova tentativa discreta em um servidor. O fallback silencioso é a pior característica que um recurso de privacidade pode ter, porque falha exatamente na direção que você estava tentando evitar e não avisa nada.

### O armazenamento é um botão, não um recurso

A etapa que as pessoas esquecem é o arquivo, porque ele aparece disfarçado de conveniência. O Cloud Sync copia os dados da sessão para os servidores do Hedy para que seus outros dispositivos possam acessá-los. Deixe-o ativado e você terá acesso entre dispositivos com processamento local. Desative-o e nada da conversa chegará aos nossos servidores, a menos que você compartilhe explicitamente essa sessão. Processamento local e armazenamento local são decisões separadas, e uma ferramenta que oferece apenas o primeiro não fechou o pipeline.

## Como verificar as alegações de um anotador?

Observe o comportamento e depois leia os documentos. Nenhum dos dois basta sozinho.

Experimente o modo avião. Desative a rede e inicie uma sessão. Se uma ferramenta continua transcrevendo e resumindo, existe um caminho local, e vale a pena saber disso. Trate o resultado como um sinal, não como prova: uma interrupção pode significar que a ferramenta exige um login ou o download de um modelo, e não a nuvem, enquanto uma ferramenta com um caminho offline funcional ainda pode encaminhar tudo por um servidor no momento em que você se reconectar. O teste diz que existe um modo local. Não diz o que acontece quando você está online.

Preste atenção à questão dos rótulos de falantes. Se uma ferramenta mostra rótulos de falantes e afirma que nada sai do seu dispositivo, pergunte qual mecanismo no dispositivo faz a diarização. Um fornecedor que consegue nomeá-lo está dizendo algo concreto. Um que não consegue pode estar identificando os falantes no servidor.

Leia a lista de subprocessadores. A política de privacidade é redigida para tranquilizar. A lista de subprocessadores existe para compras e avisos contratuais, por isso identifica as empresas no caminho. A do Hedy tem dezesseis entradas em trust.hedy.ai (https://trust.hedy.ai) . Na lista de qualquer fornecedor, verifique quais empresas podem receber conteúdo das reuniões e por quê; o tamanho da lista, por si só, diz pouco.

Pergunte o que sobrevive à exclusão. Danielle Kays, sócia da Fisher Phillips, observou que os metadados da reunião podem permanecer com um fornecedor depois que o conteúdo é excluído e que, em alguns casos, o conteúdo ingerido pode ser memorizado ou reproduzido por um modelo. A semântica de exclusão varia conforme o fornecedor, e "excluir" muitas vezes significa "remover da visualização que você consegue ver".

Se isso realmente importar, inspecione o tráfego. Testes offline e páginas de privacidade respondem a perguntas diferentes, e nenhum dos dois observa a rede. Para uma implantação regulamentada, a inspeção de pacotes ou de DNS é a verificação que observa de fato o que uma ferramenta envia.

## O que perguntar antes de instalar uma ferramenta?

Cinco perguntas. A resposta a cada uma deve ser específica.

1. Onde cada uma das três etapas é executada? Transcrição, análise e armazenamento, mencionados separadamente. Não apenas "é privado?".
2. Vocês criam rótulos de falantes e onde isso acontece? Se for no servidor, pergunte o que é o embedding, por quanto tempo ele é mantido e qual aviso os participantes recebem.
3. Qual é o cronograma de retenção e destruição? Por escrito e com um prazo. Illinois exige exatamente isso e, segundo os advogados citados mais adiante, a maioria das empresas que implanta essas ferramentas não tem esse cronograma.
4. Quem são os subprocessadores e onde estão? Essa também é a questão do GDPR (/pt/post/gdpr-checklist-ai-meeting-tools/) se você tem participantes europeus, contexto em que desenvolvimentos recentes sobre transferências UE-EUA (/pt/post/eu-us-data-transfers-supreme-court-ftc-ruling/) tornaram a base jurídica menos confortável do que antes.
5. A ferramenta faz fallback para a nuvem em caso de falha e informa isso? O fallback silencioso transforma uma configuração de privacidade em decoração.

## Como usar Hedy sem que nada saia do dispositivo?

Verifique um padrão e depois altere duas configurações.

Abra Configurações !’ Fala e IA . Confirme que Whisper ou Nemotron está selecionado. Whisper já é o padrão, portanto a maioria das pessoas encontra essa parte pronta; você só precisa mexer nela se alguém tiver trocado para um provedor na nuvem.

Na mesma tela, ative o Processamento de IA Local e escolha um modelo com o rótulo "Ótima compatibilidade". Hedy verifica a memória disponível e marca cada modelo como Ótima compatibilidade, No limite ou Não cabe, para que você não precise adivinhar. A configuração é específica de cada dispositivo, portanto seu Mac e seu iPhone precisam ser configurados separadamente.

Depois, desative o Cloud Sync . Com ele desativado, nenhum dado da reunião chega aos nossos servidores, a menos que você compartilhe explicitamente uma sessão.

Se o seu hardware não consegue rodar um modelo local, o controle de privacidade da Análise de IA em Nuvem (/pt/help/cloud-ai-analysis-privacy-control/) é o caminho intermediário: ele interrompe a análise na nuvem enquanto a transcrição local continua funcionando, para que você tenha uma transcrição privada sem notas geradas por IA. Nosso guia de configurações (/pt/post/ai-meeting-privacy-settings-explained/) cobre a matriz completa, e a página de segurança (/pt/security/) documenta cada configuração.

## Um anotador privado ainda exige consentimento?

Sim. Uma ferramenta baseada no dispositivo é mais difícil de ser vista pelas outras pessoas do que um bot.

A AP observou que os participantes podem usar dispositivos pessoais para fazer anotações, separados da plataforma de reunião, "caso em que os outros participantes não necessariamente saberiam que uma conversa estava sendo gravada e transcrita". Um bot aparece na lista de participantes. Um app no celular de alguém não mostra nada. Isso torna a gravação discreta mais fácil, e é uma crítica justa à categoria da qual fazemos parte. Thorin Klosowski, analista sênior de segurança e privacidade da Electronic Frontier Foundation, deu a resposta direta: "Pedir o consentimento de todos antes de realizar uma reunião delicada seria a abordagem mais educada."

O processamento local determina para onde os dados vão. Não diz nada sobre o consentimento das pessoas. As leis de gravação, a política do local de trabalho e os deveres profissionais continuam valendo independentemente da arquitetura, e usar uma ferramenta que ninguém consegue ver aumenta a obrigação de avisar.

O que fica mais fácil é a conversa. A maior parte da resistência a ser gravado não é sobre as notas, mas sobre o arquivo: quem mais verá isso, por quanto tempo existirá, o que acontecerá quando o fornecedor for adquirido. "Fica no meu laptop e eu vou excluir depois" é uma conversa diferente de "está sendo enviado a um serviço cujos termos eu não li". Escrevemos scripts de consentimento palavra por palavra (/pt/post/ask-permission-to-record-meeting-consent-scripts/) para a versão desconfortável, e nosso artigo sobre leis de gravação e consentimento (/pt/help/recording-laws-and-consent/) cobre a questão jurisdicional.

Chris Pluymers, advogado associado da The Dillon Law Group, também sugeriu uma forma de recusar um anotador: "Prefiro que esta reunião aconteça sem ferramentas de gravação ou transcrição com IA, e terei prazer em fazer minhas próprias anotações e compartilhar uma recapitulação, se isso ajudar." Amy Dufrane, presidente-executiva do órgão de certificação de RH HRCI, sugeriu tornar a objeção institucional, não pessoal, citando a política da empresa para que nenhum indivíduo precise ser o único a se opor.

## Por que transcrições são mais arriscadas do que gravações?

Klosowski fez a observação mais incisiva da matéria da AP: "Armazenar um monte de vídeos não é fácil, custa caro e é difícil pesquisar neles, mas o texto é muito mais fácil de pesquisar e mais barato de armazenar."

Antes dos anotadores com IA, a proteção prática de uma gravação era o atrito. Uma reunião de duas horas é um objeto de duas horas. Ninguém percorre esse conteúdo sem um motivo, e o armazenamento custa o suficiente para que as gravações sejam excluídas. Esse atrito fazia um trabalho real de segurança para o qual ninguém precisava reservar orçamento.

As transcrições eliminam esse atrito. O texto é barato o suficiente para ser mantido para sempre e pode ser pesquisado assim que chega. Uma única consulta em quatro anos de arquivos revela todas as ocorrências de uma frase para qualquer pessoa com acesso, incluindo a parte adversa com uma ordem de produção de provas. Um comentário que teria morrido em uma gravação nunca assistida se torna um resultado de busca.

Mas não se trata de um aumento inequívoco do perigo. O áudio carrega elementos que o texto perde: tom, conversas de fundo e uma amostra suficiente da sua voz para cloná-la. O áudio também pode ser transcrito mais tarde, portanto uma gravação é uma transcrição que ainda não aconteceu. A mudança vai de "alguém talvez encontre isto" para "alguém pode encontrar isto na mesma hora", e a maioria das pessoas nunca considerou essa diferença.

# O que é uma impressão vocal e quem tem a sua?

Pluymers descreveu o mecanismo: para diferenciar o Falante 1 do Falante 2, muitos anotadores derivam uma assinatura acústica de cada voz. Esse processo se chama diarização, e é o ponto que a maioria dos leitores provavelmente não considerou.

## O que diz a legislação atual

Em Illinois, impressões vocais são identificadores biométricos de acordo com a Biometric Information Privacy Act, que exige aviso por escrito, divulgação da finalidade e do prazo de retenção, uma autorização formal antes da coleta e um cronograma documentado de destruição ( 740 ILCS 14/15 (https://www.ilga.gov/ftp/ILCS/Ch%200740/Act%200014/074000140K15.html) ). A questão de um embedding de diarização se enquadrar nessa definição é uma teoria emergente que está sendo testada nos tribunais, não um ponto pacificado ( Lewis Rice (https://www.lewisrice.com/publications/ai-transcription-tools-give-rise-to-bipa-claims) ). Alguns diarizadores de ponta a ponta nem sequer funcionam dessa forma: eles mapeiam o áudio para índices anônimos de falantes sem criar um modelo persistente.

Os processos são reais. Ferramentas de IA para reuniões são um alvo ativo de ações coletivas com base na BIPA ( Fisher Phillips (https://www.fisherphillips.com/en/insights/insights/ai-meeting-tools-are-the-latest-target-of-illinois-bipa-class-actions) ), e a Fireflies.ai é ré em uma proposta de ação coletiva que alega que a empresa grava, transcreve e armazena as vozes dos participantes, inclusive de pessoas que nunca se cadastraram, sem os avisos, o consentimento e as salvaguardas de retenção exigidos ( Jackson Lewis (https://www.workplaceprivacyreport.com/2026/04/articles/artificial-intelligence/ai-meeting-assistants-and-biometric-privacy-governance-lessons-from-the-fireflies-ai-lawsuit/) ). Essas são alegações, e nenhum tribunal decidiu o mérito.

## O que uma impressão vocal roubada pode e não pode fazer

A versão assustadora circula, por isso vale corrigi-la: um embedding de diarização roubado não é uma chave da sua conta bancária. Os bancos registram os próprios modelos de voz, e o embedding interno de um fornecedor não é intercambiável com eles. O risco real ligado à voz é mais comum, e já é suficiente: ter áudio gravado em quantidade suficiente para clonar alguém de maneira convincente ( FTC (https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/04/approaches-address-ai-enabled-voice-cloning) ). Esse é um argumento sobre o áudio, não sobre o embedding.

## Por que a diarização no dispositivo muda a exposição

A diarização no dispositivo tem um precedente útil. Em Barnett v. Apple , um tribunal de apelação de Illinois confirmou a rejeição de uma ação coletiva baseada na BIPA envolvendo Face ID e Touch ID, concluindo que a Apple não possuía nem coletava os dados biométricos dos usuários porque eles nunca saíam dos próprios dispositivos, nunca eram enviados aos servidores da Apple e os recursos eram opcionais e podiam ser excluídos ( Duane Morris (https://blogs.duanemorris.com/classactiondefense/2023/01/09/illinois-appellate-court-affirms-dismissal-of-bipa-class-action-lawsuit/) , IAPP (https://iapp.org/news/b/court-rules-apples-facial-fingerprint-tools-comply-with-bipa) ). Isso corresponde de perto à diarização local: derivada no seu dispositivo, nunca transmitida, opcional e passível de exclusão. O mecanismo Nemotron (/pt/post/nemotron-on-device-speech-engine/) do Hedy funciona dessa forma.

Não é um porto seguro. Barnett dependeu dos fatos do caso, um design ou uma alegação diferente poderia levar a outro resultado, e a decisão não diz nada sobre as obrigações de quem convocou a reunião. Trata-se de redução de risco apoiada por um bom precedente, e nada disso é aconselhamento jurídico.

## Um anotador pode afetar o sigilo advogado-cliente?

Um tribunal federal decidiu que documentos gerados por IA não estavam protegidos por sigilo.

### O que o tribunal decidiu

Em United States v. Heppner , o juiz Jed Rakoff, do Southern District of New York, decidiu em fevereiro de 2026 que os documentos produzidos por um réu criminal ao inserir em um chatbot informações recebidas de seus advogados não estavam protegidos nem pelo sigilo advogado-cliente nem pela doutrina de work product. A ferramenta gerou 31 documentos a partir de seus prompts, incluindo um esboço da própria estratégia de defesa ( Harvard Law Review (https://harvardlawreview.org/blog/2026/03/united-states-v-heppner/) ). Rakoff apresentou três razões: o chatbot "claramente não é um advogado"; os próprios avisos da ferramenta alertavam contra tratar o resultado como aconselhamento jurídico, enfraquecendo qualquer alegação de que o aconselhamento jurídico era a finalidade predominante; e a política de privacidade publicada pelo fornecedor alertava que as informações do usuário poderiam ser compartilhadas em litígios, portanto o usuário não tinha uma expectativa razoável de privacidade ( Dorsey (https://www.dorsey.com/newsresources/publications/client-alerts/2026/2/ai-attorney-client-privilege) ).

O ponto do meio merece uma segunda leitura. A política de privacidade não foi a defesa. Foi a prova. O documento que o fornecedor escreveu para descrever as próprias práticas de dados se tornou o motivo pelo qual a expectativa de confidencialidade do usuário não era razoável.

### Até onde essa decisão se aplica

Heppner não decidiu se um anotador de reuniões implica renúncia ao sigilo. O caso envolvia um réu usando um chatbot por iniciativa própria, não uma ferramenta presente em uma conversa protegida por sigilo, e especialistas ainda estão avaliando o que isso significa para os anotadores ( Columbia Blue Sky (https://clsbluesky.law.columbia.edu/2026/06/16/cahill-discusses-a-i-note-takers-in-corporate-meetings/) ). A New York City Bar tem um parecer formal sobre a ética da gravação e transcrição com IA de conversas com clientes que trata a gravação e a retenção como problemas separados ( NYC Bar Formal Op. 2025-6 (https://www.nycbar.org/reports/formal-opinion-2025-6-ethical-issues-affecting-use-of-ai-to-record-transcribe-and-summarize-conversations-with-clients/) ).

O alerta mais restrito ainda se aplica: enviar material confidencial a terceiros pode enfraquecer a expectativa de que ele permanecerá confidencial. Um pipeline sem terceiros não levanta essa questão. Também não cria sigilo, impede a produção de provas ou torna adequada uma conversa gravada de forma indevida. Daniels apresentou a versão prática de forma direta: "se os dados forem para qualquer outro lugar e eles não souberem disso, aquela conversa protegida pelo sigilo advogado-cliente talvez deixe de estar protegida."

## Quais reuniões precisam de uma configuração totalmente local?

Não são todas, e fingir o contrário torna fácil descartar este conselho.

Para uma reunião semanal de acompanhamento, o padrão na nuvem é adequado. A configuração totalmente local compensa o resumo mais lento quando a própria transcrição é o risco: consultas jurídicas, investigações de RH, reuniões de diretoria e negociações, entrevistas com fontes em que um nome na transcrição pode custar o emprego de alguém e pacientes gravando as próprias consultas médicas para rever mais tarde o que o médico disse. Se você quer uma visão mais ampla das ferramentas no dispositivo para além das reuniões, comparamos sete ferramentas de IA local (/pt/post/best-local-ai-tools-for-productivity/) .

A escolha certa deve ser feita por reunião, não por pessoa. A maioria das reuniões pode usar o padrão na nuvem. Para as poucas em que a própria transcrição seria prejudicial, use uma configuração totalmente local, verifique-a antes da chamada e diga o que você está usando.

# Perguntas frequentes

## É possível usar um anotador com IA sem enviar nada para a nuvem?

Sim, mas apenas com o pequeno número de ferramentas capazes de executar todas as etapas no seu hardware. Um anotador transcreve seu áudio, analisa a transcrição e armazena o resultado. Cada uma dessas etapas pode vazar dados de forma independente, e a maioria das ferramentas executa as três nos servidores de outra empresa. Hedy transcreve no dispositivo por padrão em todas as plataformas em que está disponível e, na maioria dos dispositivos atuais, também pode executar a análise no dispositivo. Com o Cloud Sync desativado, nenhum dado da reunião chega aos nossos servidores, a menos que você compartilhe explicitamente uma sessão.

## Basta verificar se o áudio nunca sai do meu dispositivo?

Não, e esse é o erro mais comum. "O áudio nunca sai" diz apenas que a transcrição é local, uma das três etapas. Uma ferramenta pode transcrever no seu dispositivo e ainda enviar a transcrição para um modelo de linguagem, que é exatamente o que Hedy faz por padrão. A transcrição é o registro palavra por palavra, então enviá-la para fora do dispositivo levanta quase todas as mesmas questões que o áudio levantaria. Pergunte sobre cada etapa, não apenas sobre o microfone.

## Anotadores com IA criam impressões vocais dos participantes da reunião?

Alguns criam, como efeito colateral de identificar quem falou. Muitos sistemas de diarização extraem um embedding acústico de cada voz para diferenciar os falantes. A questão de esse embedding ser uma impressão vocal regulamentada pela Illinois Biometric Information Privacy Act é uma teoria jurídica em discussão, não um ponto pacificado, e nem todo sistema funciona dessa maneira. O que você pode controlar é onde a identificação acontece: a diarização no dispositivo não transmite nada.

## O processamento no dispositivo elimina a exposição relacionada à privacidade biométrica?

Ele a reduz, e há jurisprudência concreta por trás disso. Em Barnett v. Apple , um tribunal de apelação de Illinois decidiu que a Apple não possuía nem coletava os dados biométricos dos usuários porque eles permaneciam nos próprios dispositivos, nunca eram enviados aos servidores da Apple e os recursos eram opcionais e podiam ser excluídos. É um precedente relevante para o processamento local, mas dependeu desses fatos específicos. Trata-se de redução de risco, não de um porto seguro, e não diz nada sobre as obrigações de quem convocou a reunião.

## Uma ferramenta de IA pode afetar o sigilo advogado-cliente?

Um tribunal federal decidiu que documentos gerados por IA não estavam protegidos por sigilo. Em United States v. Heppner , o juiz Jed Rakoff concluiu que os documentos produzidos por um réu ao inserir em um chatbot informações recebidas de seus advogados não estavam protegidos nem pelo sigilo advogado-cliente nem pela doutrina de work product, em parte porque a política de privacidade do fornecedor alertava que as informações poderiam ser compartilhadas em litígios. Esse caso envolveu um chatbot usado pelo próprio réu, não um anotador de reuniões, portanto não resolve a questão dos anotadores. Consulte seu próprio advogado.

## Desativar o Cloud Sync torna um anotador privado?

Não por si só. A sincronização determina o armazenamento, não o processamento. Uma ferramenta pode não manter nada nos próprios servidores e ainda assim ter enviado seu áudio para uma API de transcrição e sua transcrição para um modelo de linguagem durante o processo. Armazenamento, transcrição e análise são questões separadas, e um fornecedor que responde apenas à questão do armazenamento não respondeu às outras.

## Como testar se um anotador funciona localmente?

O modo avião é uma primeira verificação útil, mas não é uma prova. Se uma ferramenta continua transcrevendo offline, existe um caminho local. Se ela para, isso pode significar que precisa da nuvem ou apenas que exige um login ou o download de um modelo. E uma ferramenta com um caminho local offline ainda pode direcionar os dados para a nuvem quando você voltar a ficar online. Combine o teste offline com a lista de subprocessadores do fornecedor e, se isso realmente importar, com uma inspeção de rede.

## A transcrição no dispositivo é precisa o suficiente para reuniões reais?

Para reuniões do dia a dia, ela funciona bem. O mecanismo Nemotron do Hedy é baseado no modelo de fala em streaming de 600 milhões de parâmetros da NVIDIA, roda inteiramente no dispositivo e identifica quem disse o quê. A precisão ainda varia conforme o sotaque, o ruído de fundo, as falas simultâneas e o vocabulário especializado, portanto teste-o nas suas próprias reuniões em vez de confiar no benchmark de qualquer pessoa, inclusive no nosso.

## Um anotador baseado no dispositivo é menos transparente do que um bot de reunião?

Sim, e isso pesa contra ferramentas como a nossa. Um bot se anuncia na lista de participantes. Um app no celular de alguém não anuncia nada, o que torna a gravação secreta mais fácil, não mais difícil. A Associated Press levantou esse ponto diretamente. O processamento local resolve para onde os dados vão e não faz nada a respeito do consentimento das pessoas. São deveres separados, e você ainda precisa cumprir o segundo.

## O que Hedy envia para a nuvem por padrão?

O reconhecimento de fala roda no seu dispositivo em todas as plataformas, portanto o áudio não sai por padrão. A etapa de análise que escreve resumos e sugestões roda na nuvem por padrão, onde o conteúdo da transcrição é processado de forma transitória e não é usado para treinar modelos. Esse padrão é uma escolha deliberada para ampliar a compatibilidade com dispositivos e a qualidade dos resultados. Você pode levar a análise para o dispositivo com o Processamento de IA Local (/pt/help/local-

ai-processing/) e desativar o Cloud Sync para que nada seja sincronizado.

## O processamento local custa mais?

Não. O reconhecimento de fala no dispositivo e o Processamento de IA Local fazem parte do produto, em vez de constituírem um nível de privacidade separado. O plano gratuito inclui 300 minutos por mês, e o Pro custa $12.99 por mês ou $99.99 por ano. Os modelos locais exigem um único download, em vez de uma cobrança por minuto, portanto o caminho totalmente local não tem custo de uso. Consulte os preços (/pt/pricing/) para ver os planos atuais.

---

Hedy AI · Coaching de IA ao vivo para conversas importantes
Experimente o Hedy grátis: https://www.hedy.ai/pt/downloads/
https://www.hedy.ai/pt/post/how-to-use-ai-meeting-notes-privately/