Votre preneur de notes IA est-il vraiment privé ?

Les preneurs de notes IA transforment votre réunion en une archive détenue par quelqu'un d'autre. Découvrez ce qui quitte votre appareil à chaque étape, comment vérifier les affirmations d'un outil et comment tout garder en local.

Publié par Julian Pscheid · 15 juillet 2026 · Mis à jour 20 août 2026
Lire cet article en ligne: https://www.hedy.ai/fr/post/how-to-use-ai-meeting-notes-privately/

Deux collègues discutent autour d'une petite table dans un bureau privé, porte fermée, avec un iPhone posé face contre table entre eux, à côté d'un carnet et d'un mug Oregon Ducks en forme de canard

Réponse rapide Un preneur de notes IA en réunion accomplit trois opérations qui peuvent chacune exposer des données : il transcrit votre audio, analyse la transcription et stocke le résultat. La plupart des outils exécutent les trois sur leurs propres serveurs. La réunion devient alors une archive consultable détenue par quelqu'un d'autre. Quelques outils peuvent exécuter ces trois opérations sur du matériel qui vous appartient. C'est la seule configuration où rien concernant la réunion ne quitte la pièce. Hedy transcrit par défaut sur l'appareil sur toutes les plateformes où il est disponible et, sur la plupart des appareils récents, peut aussi exécuter l'analyse sur l'appareil. Si vous désactivez également Cloud Sync dans Hedy, rien de la conversation n'arrive sur nos serveurs, à moins que vous ne partagiez explicitement cette session.

The Associated Press a publié ce mois-ci un article sur les preneurs de notes IA au travail qui dresse un bon inventaire des risques (AP, juillet 2026 (https://apnews.com/article/ai-notetaker-work-meetings-privacy-data-c700299371ca7cfec77dafdfb948067f)) : informations confidentielles sur le personnel, stratégie d'entreprise, secrets commerciaux, remarques qui pourraient être mal interprétées lors d'une

déposition ultérieure. Ses conseils sont également sensés. Vérifiez si un preneur de notes a rejoint la réunion. Demandez le consentement avant une réunion sensible. Appuyez-vous sur la politique de l'entreprise afin qu'aucune personne n'ait à être celle qui s'y oppose. Désactivez l'outil pendant la partie délicate. Demandez ce que le fournisseur conserve et s'il utilise ces données pour l'entraînement.

Chacune de ces mesures gère les conséquences de la transformation de votre réunion en une archive détenue par quelqu'un d'autre. Aucune ne demande si cette transformation est nécessaire. Justin Daniels, avocat d'affaires chez Baker Donelson, a livré à l'article sa formule la plus percutante : « Je ne commencerai pas à parler de quoi que ce soit de substantiel tant que l'outil ne sera pas désactivé, car je ne veux tout simplement pas prendre ce risque. » C'est le bon conseil pour les outils dont disposent la plupart des gens, et il part du principe que la réunion doit quitter votre matériel.

Sur les appareils actuels, ce n'est pas nécessaire. Quelques produits peuvent exécuter toute la chaîne de traitement sur votre propre machine, et presque personne ne le sait.

Qu'est-ce qui quitte votre appareil quand vous utilisez un preneur de notes ?

Trois éléments, qui peuvent exposer des données indépendamment. La transcription transforme votre audio en texte. L'analyse lit ce texte et rédige votre résumé ainsi que vos actions à mener. Le stockage détermine si une partie de ces données persiste quelque part hors de votre contrôle. Chaque étape peut rester sur du matériel qui vous appartient ou passer sur celui de quelqu'un d'autre, ce qui donne huit combinaisons possibles.

Étape	Ce qu'elle fait	Peut-elle s'exécuter sur l'appareil ?	Ce qui quitte l'appareil dans le cas contraire
Transcription	Transforme l'audio en texte, parfois avec des étiquettes de locuteur	Oui, sur le matériel actuel	L'audio lui-même, ainsi qu'un embedding acoustique par locuteur dans de nombreux systèmes
Analyse	Lit la transcription, rédige les résumés et les actions à mener	Oui, sur du matériel compatible	La transcription et tout ce qu'un modèle en déduit
Stockage et synchronisation	Conserve l'archive	Oui, s'ils restent désactivés	Une copie durable et consultable, ainsi que des métadonnées qui peuvent subsister après la suppression

C'est ici que se cachent la plupart des affirmations en matière de confidentialité. « L'audio ne quitte jamais votre appareil » ressemble à une affirmation concernant l'ensemble du produit. Cela signifie seulement que la transcription est locale, et n'empêche pas l'envoi de la transcription verbatim intégrale à un modèle de langage une seconde plus tard. C'est précisément ce que fait Hedy par défaut. Voilà pourquoi demander si l'audio quitte l'appareil ne suffit pas. La transcription constitue l'archive. Une fois qu'elle a quitté votre machine, l'essentiel de ce qui vous préoccupait a quitté votre machine avec elle.

Le traitement hybride est courant, y compris dans la configuration par défaut de Hedy. Le problème, c'est un fournisseur qui refuse de dire quelles étapes quittent votre appareil.

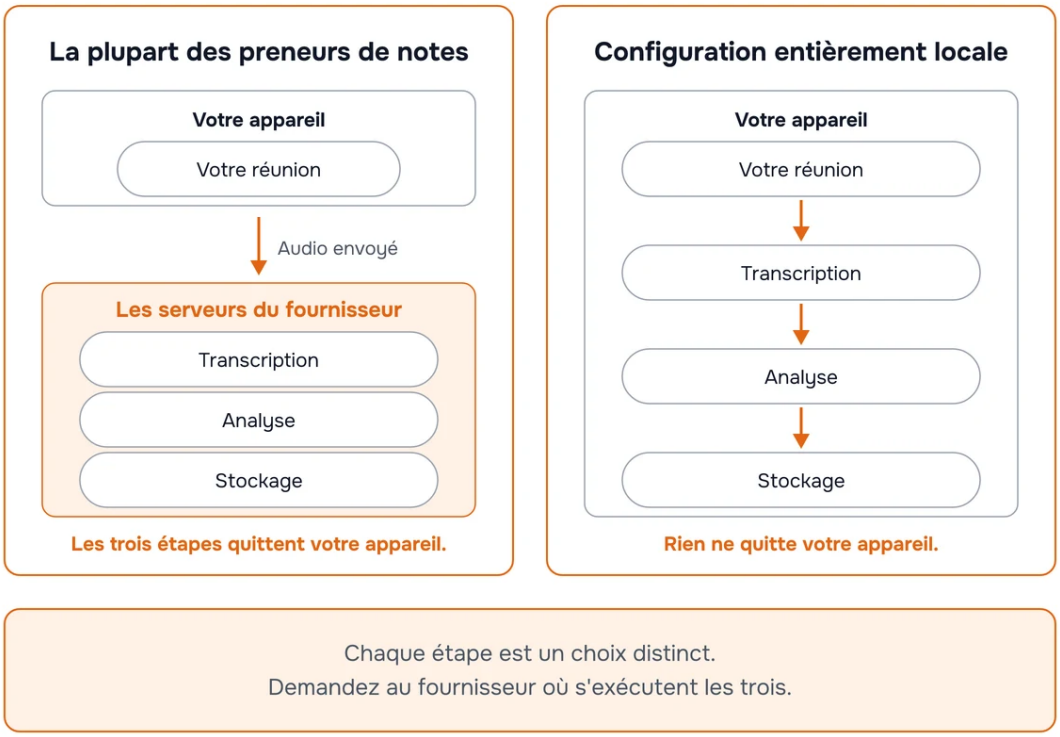

Schéma comparant la plupart des preneurs de notes, où l'audio est envoyé aux serveurs du fournisseur et où la transcription, l'analyse et le stockage s'y déroulent, à une configuration entièrement locale où les trois étapes s'exécutent sur votre propre appareil

Toute la chaîne de traitement peut-elle s'exécuter sur votre appareil ?

Oui, sur le matériel actuel, et c'est ce qui a discrètement changé. Très peu de produits exécutent les trois étapes sur l'appareil.

La transcription est l'étape la plus simple

Whisper, le moteur par défaut, fonctionne sur toutes les plateformes où Hedy est disponible. Nemotron fonctionne sur toutes les plateformes natives, mais pas dans l'application web. Nemotron est un moteur en streaming fondé sur le modèle vocal de NVIDIA à 600 millions de paramètres (https://huggingface.co/nvidia/nemotron-3.5-asr-streaming-0.6b) , et il ajoute les étiquettes de locuteur qui poussaient auparavant les utilisateurs vers un moteur cloud. Il nécessite un téléchargement unique d'environ 0,6 à 0,7 Go et un matériel datant au moins de la génération de l'iPhone 12. La précision varie toujours selon l'accent, le bruit ambiant, les paroles qui se chevauchent et le vocabulaire spécialisé. Testez-le donc sur vos propres réunions plutôt que de vous fier à un chiffre publié.

C'est au stade de l'analyse que se situe le compromis

Le Traitement IA local (/fr/help/local-ai-processing/) exécute les résumés et les suggestions sur votre machine. Il nécessite un matériel performant : un Mac Apple Silicon, un PC Windows équipé d'un GPU adapté, ou un iPhone ou iPad récent. La taille des modèles va d'environ 1,2 Go pour la catégorie mobile à plus de 20 Go. Un modèle intermédiaire d'environ 9 milliards de paramètres fonctionne confortablement sur un Mac doté de 16 Go de mémoire. Les plus grands modèles demandent environ 25 Go de RAM ou davantage.

Le Traitement IA local est désactivé par défaut, car l'analyse cloud est plus rapide et produit actuellement de meilleurs résultats. La configuration par défaut de Hedy repose sur une séparation délibérée : la reconnaissance vocale s'exécute localement partout afin que l'audio ne quitte jamais l'appareil sans que vous l'ayez demandé, tandis que l'analyse s'exécute dans le cloud afin que le produit fonctionne correctement sur du matériel incapable d'héberger un modèle de langage. Un résumé qui semble instantané dans le cloud peut prendre de trente secondes à plusieurs minutes en local. Notre analyse technique approfondie (/fr/post/local-ai-engineering-deep-dive-hedy-3-2/) présente tous les détails.

Le Traitement IA local ne bascule pas silencieusement vers le cloud. Si une opération échoue en local, vous obtenez une erreur, pas une nouvelle tentative discrète sur un serveur. Le fallback silencieux est la pire propriété qu'une fonction de confidentialité puisse avoir : il échoue précisément dans la direction que vous cherchiez à éviter et ne vous en informe pas.

Le stockage est un réglage, pas une fonctionnalité

L'étape que les utilisateurs oublient est l'archive, parce qu'elle se présente sous les traits de la commodité. Cloud Sync copie les données de session sur les serveurs de Hedy afin que vos autres appareils puissent y accéder. Laissez-le activé et vous bénéficiez d'un accès sur plusieurs appareils avec un traitement local. Désactivez-le et rien de la conversation n'arrive sur nos serveurs, à moins que vous ne partagiez explicitement cette session. Le traitement local et le stockage local sont deux décisions distinctes. Un outil qui ne propose que le premier n'a pas fermé toute la chaîne.

Comment vérifier les affirmations d'un preneur de notes ?

Observez son comportement, puis lisez les documents. Ni l'un ni l'autre ne suffit à lui seul.

Essayez le mode avion. Désactivez le réseau et démarrez une session. Si un outil continue à transcrire et à résumer, un chemin de traitement local existe, ce qui est utile à savoir. Considérez ce résultat comme un indice, et non comme une preuve : un blocage peut signifier que l'outil attend une connexion au compte ou le téléchargement d'un modèle plutôt que le cloud, et un outil disposant d'un chemin hors ligne fonctionnel peut tout envoyer par un serveur dès que vous vous reconnectez. Le test vous indique qu'un mode local existe. Il ne vous dit pas ce qui se passe quand vous êtes en ligne.

Examinez la question des étiquettes de locuteur. Si un outil affiche des étiquettes de locuteur et affirme que rien ne quitte votre appareil, demandez quel moteur sur l'appareil réalise la diarisation. Un fournisseur capable de le nommer vous donne une information concrète. Un fournisseur qui en est incapable effectue peut-être l'identification côté serveur.

Lisez la liste des sous-traitants. La politique de confidentialité est rédigée pour rassurer. La liste des sous-traitants sert aux achats et aux notifications contractuelles, et nomme donc les entreprises qui interviennent dans la chaîne. Celle de Hedy compte seize entrées sur trust.hedy.ai (https://trust.hedy.ai) . Pour n'importe quel fournisseur, consultez cette liste afin de savoir quelles entreprises peuvent recevoir le contenu des réunions et pourquoi. Sa longueur seule ne vous apprend pas grand-chose.

Demandez ce qui subsiste après la suppression. Danielle Kays, associée chez Fisher Phillips, a fait remarquer que les métadonnées des réunions peuvent rester chez un fournisseur après la suppression du contenu et que le contenu ingéré peut, dans certains cas, être mémorisé ou reproduit par un modèle. Les modalités de suppression varient selon le fournisseur, et « supprimer » signifie souvent « retirer de la vue à laquelle vous avez accès ».

Si l'enjeu le justifie vraiment, inspectez le trafic. Les tests hors ligne et les pages de confidentialité répondent à des questions différentes, et aucun des deux n'observe le réseau. Pour un déploiement réglementé, l'inspection des paquets ou du DNS est le contrôle qui permet réellement d'observer ce qu'envoie un outil.

Quelles questions poser avant d'en installer un ?

Cinq questions. Chacune doit recevoir une réponse précise.

1. Où s'exécute chacune des trois étapes ? La transcription, l'analyse et le stockage doivent être nommés séparément. Ne demandez pas simplement si l'outil est privé.

2. Créez-vous des étiquettes de locuteur, et où ? Si elles sont créées côté serveur, demandez ce qu'est l'embedding, combien de temps il est conservé et quelles informations les participants reçoivent.

3. Quel est le calendrier de conservation et de destruction ? Exigez une réponse écrite avec une durée. C'est exactement ce que demande l'Illinois et, d'après les avocats cités plus loin, la plupart des entreprises qui déploient ces outils n'en ont pas.

4. Qui sont les sous-traitants, et où se trouvent-ils ? C'est aussi la question du RGPD (/fr/post/gdpr-checklist-ai-meeting-tools/) si vous avez des participants européens. Les évolutions récentes concernant les transferts UE-US (/fr/post/eu-us-data-transfers-supreme-court-ftc-ruling/) ont rendu leur fondement juridique moins confortable qu'auparavant.

5. L'outil bascule-t-il vers le cloud en cas d'échec, et vous en informe-t-il ? Un fallback silencieux transforme un réglage de confidentialité en décoration.

Comment utiliser Hedy sans que rien ne quitte votre appareil ?

Vérifiez un réglage par défaut, puis modifiez-en deux.

Ouvrez Settings !’ Speech & AI . Vérifiez que Whisper ou Nemotron est sélectionné. Whisper est déjà le choix par défaut, donc la plupart des utilisateurs n'ont rien à faire. Vous ne devez modifier ce réglage que si quelqu'un l'a remplacé par un fournisseur cloud.

Sur le même écran, activez Local AI Processing et choisissez un modèle portant le label « Great fit ». Hedy vérifie la mémoire disponible et classe chaque modèle comme Great fit, Tight fit ou Won't fit. Vous n'avez donc pas à deviner. Le réglage s'applique par appareil : votre Mac et votre iPhone doivent chacun être configurés séparément.

Désactivez ensuite Cloud Sync . Une fois ce réglage désactivé, aucune donnée de réunion n'arrive sur nos serveurs, à moins que vous ne partagiez explicitement une session.

Si votre matériel ne peut pas exécuter de modèle local, le contrôle de confidentialité de l'analyse IA cloud (/fr/help/cloud-ai-analysis-privacy-control/) constitue une solution intermédiaire : il arrête l'analyse cloud tandis que la transcription locale continue de fonctionner. Vous obtenez ainsi une transcription privée sans notes générées par IA. Notre guide des paramètres (/fr/post/ai-meeting-privacy-settings-explained/) couvre toutes les configurations, et la page Sécurité (/fr/security/) documente chacune d'elles.

Un preneur de notes privé nécessite-t-il toujours le consentement ?

Oui. Un outil sur l'appareil est plus difficile à voir pour les autres personnes qu'un bot.

AP a relevé que les participants peuvent utiliser des appareils de prise de notes personnels distincts de la plateforme de réunion, « auquel cas les autres participants ne sauraient pas nécessairement qu'une discussion est enregistrée et transcrite ». Un bot apparaît dans la liste des participants. Une application sur le téléphone de quelqu'un n'affiche rien. Cela facilite l'enregistrement discret, et c'est une critique légitime de la catégorie à laquelle nous appartenons. Thorin Klosowski, analyste principal en sécurité et confidentialité à l'Electronic Frontier Foundation, a donné la réponse la plus simple : « Demander le consentement de tout le monde avant une réunion sensible serait l'approche la plus courtoise. »

Le traitement local détermine où vont les données. Il ne dit rien sur le consentement des personnes. Le droit de l'enregistrement, les politiques de l'entreprise et les obligations professionnelles restent applicables quelle que soit l'architecture. Et l'utilisation d'un outil que personne ne peut voir renforce l'obligation de l'annoncer.

Ce qui devient plus simple, c'est la conversation. La plupart des réticences à l'enregistrement ne concernent pas les notes, mais l'archive : qui d'autre peut la voir, combien de temps elle existe et ce qui se passe si le fournisseur est racheté. « Les données restent sur mon ordinateur portable et je les supprimerai ensuite » ouvre une autre conversation que « elles sont téléversées vers un service dont je n'ai pas lu les conditions ». Nous avons rédigé des scripts de consentement mot pour mot (/fr/post/ask-permission-to-record-meeting-consent-scripts/) pour cette situation délicate, et notre article sur les lois et le consentement pour enregistrer une conversation (/fr/help/recording-laws-and-consent/) aborde la question des juridictions.

Chris Pluymers, avocat associé chez The Dillon Law Group, a également proposé une formule pour refuser un preneur de notes : « Je préfère que cette réunion se déroule sans outils d'enregistrement ou de transcription par IA. Je serais heureux de prendre mes propres notes et de partager un récapitulatif si cela peut être utile. » Amy Dufrane, directrice générale de l'organisme de certification RH HRCI, a suggéré d'en faire une règle institutionnelle plutôt qu'une objection personnelle, en invoquant la politique de l'entreprise afin qu'aucune personne n'ait à être celle qui s'y oppose.

Pourquoi les transcriptions sont-elles plus risquées que les enregistrements ?

Klosowski a formulé l'observation la plus juste dans l'article d'AP : « Stocker une grande quantité de vidéos n'est pas simple : c'est coûteux et difficile à parcourir. Le texte, en revanche, est bien plus facile à rechercher et moins cher à stocker. »

Avant les preneurs de notes IA, la friction offrait une protection pratique aux enregistrements. Une réunion de deux heures est un objet de deux heures. Personne ne la parcourt sans raison, et son stockage coûte assez cher pour que les enregistrements finissent par être supprimés. Cette friction accomplissait un véritable travail de sécurité sans qu'aucun budget lui soit consacré.

Les transcriptions la suppriment. Le texte coûte assez peu cher pour être conservé indéfiniment et peut être recherché dès son arrivée. Une seule requête dans quatre années d'archives fait ressortir chaque occurrence d'une expression pour toute personne disposant d'un accès, y compris la partie adverse munie d'une ordonnance de communication de pièces. Une remarque qui aurait disparu dans un enregistrement jamais visionné devient un résultat de recherche.

Le danger n'augmente toutefois pas de manière uniforme. L'audio contient des éléments que le texte perd : le ton, les conversations en arrière-plan et une quantité suffisante de votre voix pour la cloner. Il peut aussi être transcrit plus tard. Un enregistrement est donc une transcription qui n'a pas encore eu lieu. On passe de « quelqu'un pourrait trouver ceci » à « quelqu'un peut trouver ceci immédiatement », et

la plupart des gens n'ont jamais pris en compte cette différence.

Qu'est-ce qu'une empreinte vocale, et qui détient la vôtre ?

Pluymers a décrit le mécanisme : pour distinguer le Locuteur 1 du Locuteur 2, de nombreux preneurs de notes dérivent une signature acoustique de chaque voix. Ce processus s'appelle la diarisation, et c'est le point auquel la plupart des lecteurs n'auront pas pensé.

État du droit

En Illinois, les empreintes vocales sont des identifiants biométriques au titre du Biometric Information Privacy Act. Cette loi exige un avis écrit, la communication de la finalité et de la durée de conservation, une autorisation signée avant la collecte et un calendrier de destruction documenté (740 ILCS 14/15 (https://www.ilga.gov/ftp/ILCS/Ch%200740/Act%200014/074000140K15.html)). La question de savoir si un embedding de diarisation entre dans cette définition relève d'une théorie émergente actuellement débattue devant les tribunaux, et non d'un droit établi (Lewis Rice (https://www.lewisrice.com/publications/ai-transcription-tools-give-rise-to-bipa-claims)). Certains systèmes de diarisation de bout en bout ne fonctionnent même pas de cette manière : ils associent l'audio à des indices de locuteur anonymes sans créer de modèle persistant.

Les litiges sont bien réels. Les outils de réunion IA sont activement visés par des actions collectives fondées sur le BIPA (Fisher Phillips (https://www.fisherphillips.com/en/insights/insights/ai-meeting-tools-are-the-latest-target-of-illinois-bipa-class-actions)), et Fireflies.ai est défendeur dans un projet d'action collective qui lui reproche d'enregistrer, de transcrire et de stocker les voix des participants, y compris de personnes qui ne se sont jamais inscrites, sans l'avis, le consentement et les garanties de conservation requis (Jackson Lewis (https://www.workplaceprivacyreport.com/2026/04/articles/artificial-intelligence/ai-meeting-assistants-and-biometric-privacy-governance-lessons-from-the-fireflies-ai-lawsuit/)). Il s'agit d'allégations, et aucun tribunal ne s'est prononcé sur le fond.

Ce qu'une empreinte vocale volée permet ou ne permet pas de faire

Une version alarmiste circule, et il convient de la corriger : un embedding de diarisation volé n'est pas une clé donnant accès à votre compte bancaire. Les banques enregistrent leurs propres modèles vocaux, et l'embedding interne d'un fournisseur n'est pas interchangeable avec eux. Le véritable risque lié à la voix est plus ordinaire, ce qui suffit : disposer d'assez d'audio enregistré pour cloner quelqu'un de manière convaincante (FTC (https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/04/approaches-address-ai-enabled-voice-cloning)). Cet argument concerne l'audio, pas l'embedding.

Pourquoi la diarisation sur l'appareil change le niveau d'exposition

La diarisation sur l'appareil bénéficie d'un précédent utile. Dans Barnett v. Apple , une cour d'appel de l'Illinois a confirmé le rejet d'une action collective fondée sur le BIPA concernant Face ID et Touch ID. Elle a estimé qu'Apple ne détenait ni ne collectait les données biométriques des utilisateurs, car elles ne quittaient jamais leurs propres appareils, n'étaient jamais envoyées aux serveurs d'Apple et les fonctionnalités étaient facultatives et supprimables (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)). Cela correspond étroitement à la diarisation locale : dérivée sur votre appareil, jamais transmise, facultative et supprimable. Le moteur Nemotron (/fr/post/nemotron-on-device-speech-engine/) de Hedy fonctionne ainsi.

Ce n'est pas une protection automatique. Barnett dépendait des faits propres à l'affaire, une conception ou des conclusions différentes pourraient mener à un autre résultat, et la décision ne dit rien des obligations de la personne qui a organisé la réunion. Il s'agit d'une réduction des risques étayée par un précédent solide, et rien de tout cela ne constitue un avis juridique.

Un preneur de notes peut-il affecter le secret professionnel avocat-client ?

Une juridiction fédérale a estimé que des documents générés par IA n'étaient pas protégés par le secret professionnel.

Ce qu'a décidé la juridiction

Dans United States v. Heppner , le juge Jed Rakoff du Southern District of New York a décidé en février 2026 que les documents qu'un prévenu avait produits en transmettant à un chatbot des informations fournies par ses avocats n'étaient protégés ni par le secret professionnel avocat-client ni par la doctrine des documents préparés en vue d'un litige. L'outil avait généré 31 documents à partir de ses prompts, dont un plan de sa propre stratégie de défense (Harvard Law Review (https://harvardlawreview.org/blog/2026/03/united-states-v-heppner/)). Rakoff a donné trois raisons : le chatbot n'est « manifestement pas un avocat » ; ses propres avertissements déconseillaient de considérer ses réponses comme des conseils juridiques, ce qui contredisait l'idée que le conseil juridique était l'objectif principal ; et la politique de confidentialité publiée par le fournisseur avertissait que les informations des utilisateurs pourraient être communiquées dans le cadre d'une procédure judiciaire. L'utilisateur ne pouvait donc pas raisonnablement s'attendre à leur confidentialité (Dorsey (https://www.dorsey.com/newsresources/publications/client-alerts/2026/2/ai-attorney-client-privilege)).

Ce dernier point mérite une deuxième lecture. La politique de confidentialité n'a pas servi de moyen de défense. Elle a constitué la preuve. Le document rédigé par le fournisseur pour décrire ses propres pratiques en matière de données est devenu la raison pour laquelle l'attente de confidentialité de l'utilisateur n'était pas raisonnable.

Jusqu'où cette décision s'applique-t-elle ?

Heppner n'a pas décidé si un preneur de notes de réunion entraîne la renonciation au secret professionnel. L'affaire concernait un prévenu utilisant un chatbot de sa propre initiative, et non un outil assistant à une conversation protégée, et les spécialistes continuent d'en examiner les conséquences pour les preneurs de notes (Columbia Blue Sky (https://clsbluesky.law.columbia.edu/2026/06/16/cahill-discusses-a-i-note-takers-in-corporate-meetings/)). Le New York City Bar a publié un avis formel sur les règles déontologiques applicables à l'utilisation de l'IA pour enregistrer et transcrire les conversations avec les clients, qui traite l'enregistrement et la conservation comme deux problèmes distincts (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/)).

Son avertissement plus limité reste pertinent : envoyer des informations confidentielles à un tiers peut affaiblir l'attente selon laquelle elles resteront confidentielles. Une chaîne de traitement sans aucun tiers ne soulève pas cette question. Elle ne crée pas non plus de secret professionnel, n'empêche pas la communication de pièces et ne rend pas licite une conversation enregistrée de manière irrégulière. Daniels a résumé la conséquence pratique sans détour : « Si les données vont ailleurs sans qu'ils le sachent, cette conversation couverte par le secret professionnel avocat-client risque de ne plus l'être. »

Quelles réunions nécessitent une configuration entièrement locale ?

Pas toutes, et prétendre le contraire rendrait ce conseil facile à écarter.

Pour une réunion de suivi hebdomadaire, la configuration cloud par défaut convient. La configuration entièrement locale vaut le résumé plus lent lorsque la transcription elle-même constitue le risque : consultations juridiques, enquêtes RH, discussions de conseil d'administration ou de transaction, interviews de sources où un nom dans une transcription peut coûter son emploi à quelqu'un, et patients enregistrant leurs propres rendez-vous médicaux pour revoir ensuite les propos du médecin. Si vous souhaitez élargir votre réflexion aux outils sur l'appareil au-delà des réunions, nous avons comparé sept outils d'IA locale (/fr/post/best-local-ai-tools-for-productivity/) .

Le bon choix se fait réunion par réunion, pas personne par personne. La plupart des réunions peuvent utiliser la configuration cloud par défaut. Pour les quelques réunions où la transcription elle-même serait préjudiciable, utilisez une configuration entièrement locale, vérifiez-la avant l'appel et annoncez ce que vous utilisez.

Questions fréquentes

Pouvez-vous utiliser un preneur de notes IA sans rien envoyer dans le cloud ?

Oui, mais seulement avec le petit nombre d'outils capables d'exécuter chaque étape sur votre matériel. Un preneur de notes transcrit votre audio, analyse la transcription et stocke le résultat. Chacune de ces étapes peut exposer des données indépendamment, et la plupart des outils exécutent les trois sur les serveurs de quelqu'un d'autre. Hedy transcrit par défaut sur l'appareil sur toutes les plateformes où il est disponible et, sur la plupart des appareils récents, peut aussi exécuter l'analyse sur l'appareil. Lorsque Cloud Sync est désactivé, aucune donnée de réunion n'arrive sur nos serveurs, à moins que vous ne partagiez explicitement une session.

Suffit-il de vérifier que l'audio ne quitte jamais mon appareil ?

Non, et c'est l'erreur la plus courante. « L'audio ne quitte jamais votre appareil » vous indique seulement que la transcription est locale, soit une étape sur trois. Un outil peut transcrire sur votre appareil tout en envoyant la transcription à un modèle de langage, ce que fait précisément Hedy par défaut. La transcription est le compte rendu verbatim : l'envoyer hors de l'appareil soulève donc presque toutes les mêmes questions que l'audio. Renseignez-vous sur chaque étape, pas seulement sur le microphone.

Les preneurs de notes IA créent-ils des empreintes vocales des participants à la réunion ?

Certains le font comme effet secondaire de l'identification des locuteurs. De nombreux systèmes de diarisation extraient un embedding acoustique de chaque voix afin de distinguer les locuteurs. La question de savoir si cet embedding constitue une empreinte vocale réglementée au titre du Biometric Information Privacy Act de l'Illinois relève d'une théorie juridique actuellement débattue, et non d'un droit établi, et tous les systèmes ne fonctionnent pas ainsi. Ce que vous pouvez contrôler, c'est l'endroit où l'identification s'effectue : la diarisation sur l'appareil ne transmet rien.

Le traitement sur l'appareil élimine-t-il les risques liés à la confidentialité biométrique ?

Il les réduit, et une véritable jurisprudence l'étaye. Dans Barnett v. Apple , une cour d'appel de l'Illinois a estimé qu'Apple ne détenait ni ne collectait les données biométriques des utilisateurs, car elles restaient sur leurs propres appareils, n'étaient jamais envoyées aux serveurs d'Apple et les fonctionnalités étaient facultatives et supprimables. C'est un précédent important pour le traitement local, mais il dépendait de ces faits précis. Il s'agit d'une réduction des risques, pas d'une protection automatique, et cette décision ne dit rien des obligations de la personne qui a organisé la réunion.

Un outil d'IA peut-il affecter le secret professionnel avocat-client ?

Une juridiction fédérale a estimé que des documents générés par IA n'étaient pas protégés par le secret professionnel. Dans United States v. Heppner , le juge Jed Rakoff a conclu que les documents qu'un prévenu avait produits en transmettant à un chatbot des informations fournies par ses avocats n'étaient protégés ni par le secret professionnel ni en tant que documents préparés en vue d'un litige, notamment parce que la politique de confidentialité du fournisseur avertissait que les informations pourraient être communiquées dans le cadre d'une procédure judiciaire. Cette affaire concernait un chatbot utilisé par le prévenu de sa propre initiative, et non un preneur de notes de réunion. Elle ne tranche donc pas la question des preneurs de notes. Consultez votre propre avocat.

Désactiver Cloud Sync rend-il un preneur de notes privé ?

Pas à lui seul. La synchronisation régit le stockage, pas le traitement. Un outil peut ne rien conserver sur ses serveurs tout en ayant envoyé votre audio à une API de transcription et votre transcription à un modèle de langage au passage. Le stockage, la transcription et l'analyse sont des questions distinctes. Un fournisseur qui ne répond qu'à celle du stockage n'a pas répondu aux autres.

Comment vérifier qu'un preneur de notes fonctionne en local ?

Le mode avion constitue un premier test utile, mais pas une preuve. Si un outil continue de transcrire hors ligne, un chemin de traitement local existe. S'il se bloque, cela peut signifier qu'il a besoin du cloud, ou simplement qu'il attend une connexion au compte ou le téléchargement d'un modèle. Et un outil disposant d'un chemin local hors ligne peut tout de même passer par le cloud dès que vous êtes de nouveau en ligne. Associez le test hors ligne à la liste des sous-traitants du fournisseur et, si l'enjeu le justifie vraiment, à une inspection du trafic réseau.

La transcription sur l'appareil est-elle assez précise pour de vraies réunions ?

Pour les réunions courantes, elle tient bien la route. Le moteur Nemotron de Hedy repose sur le modèle vocal en streaming de NVIDIA à 600 millions de paramètres, s'exécute entièrement sur l'appareil et indique qui a dit quoi. La précision varie toujours selon l'accent, le bruit de fond, les paroles qui se chevauchent et le vocabulaire spécialisé. Testez-le donc sur vos propres réunions plutôt que de vous fier au benchmark de qui que ce soit, y compris au nôtre.

Un preneur de notes sur l'appareil est-il moins transparent qu'un bot de réunion ?

Oui, et c'est un point qui joue contre des outils comme le nôtre. Un bot s'annonce dans la liste des participants. Une application sur le téléphone de quelqu'un ne signale rien, ce qui rend l'enregistrement secret plus facile, pas plus difficile. The Associated Press a soulevé directement ce problème. Le

traitement local détermine où vont les données, mais ne change rien au consentement des personnes. Ce sont deux obligations distinctes, et vous devez toujours respecter la seconde.

Qu'est-ce que Hedy envoie par défaut dans le cloud ?

La reconnaissance vocale s'exécute sur votre appareil sur toutes les plateformes, de sorte que l'audio ne le quitte pas par défaut. L'étape d'analyse qui rédige les résumés et les suggestions s'exécute par défaut dans le cloud, où le contenu de la transcription est traité de manière transitoire et n'est pas utilisé pour entraîner des modèles. Ce choix par défaut est un compromis délibéré entre la prise en charge d'un large éventail d'appareils et la qualité des résultats. Vous pouvez déplacer l'analyse sur l'appareil avec le Traitement IA local (/fr/help/local-ai-processing/) et désactiver Cloud Sync pour empêcher toute synchronisation.

Le traitement local coûte-t-il plus cher ?

Non. La reconnaissance vocale sur l'appareil et le Traitement IA local font partie du produit, et non d'une offre de confidentialité distincte. L'offre gratuite comprend 300 minutes par mois et Pro coûte $12.99 par mois ou $99.99 par an. Les modèles locaux se téléchargent une seule fois et ne sont pas facturés à la minute : la configuration entièrement locale n'entraîne donc aucun coût d'utilisation. Consultez les tarifs (/fr/pricing/) actuels.

Hedy AI · Coaching IA en direct pour les conversations importantes
Essayez Hedy gratuitement: https://www.hedy.ai/fr/downloads/
https://www.hedy.ai/fr/post/how-to-use-ai-meeting-notes-privately/