

Privacy Policy

Version	2026-10-16
Effective	October 16, 2026
Supersedes	the version dated October 7, 2026
First published	August 6, 2026
Operated by	Any Percent LLC, a Washington limited liability company, doing business as Psybird.ai

1. Introduction and scope

Psybird.ai is operated by Any Percent LLC, a Washington limited liability company, doing business as Psybird.ai (“Psybird,” “we,” “our,” or “us”). Psybird provides an AI-supported platform that helps licensed health care professionals, including mental health clinicians and physical therapists, extend clinician-directed support to their clients between sessions and visits. Psybird is not a healthcare provider, clinician, crisis service, or a replacement for professional treatment.

This Privacy Policy explains how we handle personal information. Because different rules apply to different data, please note which framework governs what:

Type of data	Governing framework	Where it is described
Protected health information (PHI) we handle for a Practice under a BAA	HIPAA and the Business Associate Agreement	The Practice's HIPAA Notice of Privacy Practices, and the BAA between Psybird and the Practice
Consumer health data of Washington residents that is not HIPAA PHI	Washington My Health My Data Act (MHMDA)	Our separate Consumer Health Data Privacy Policy (see Section 12)
Other personal data (e.g., website visitors, clinician accounts, technical data)	This Privacy Policy and applicable state privacy laws	This document

2. Our role: business associate and data controller

When we handle PHI on behalf of a Practice, we act as that Practice's HIPAA business associate, and the Practice (the covered entity) remains responsible for its own HIPAA obligations. For personal data that is not PHI (such as data from website visitors, prospective users, and clinician account and technical data), we act as a controller (or, under some state laws, a processor) and this Policy applies. The same underlying data can shift between these regimes, so we apply the protections appropriate to each.

3. Information we collect

3.1 Client information

Depending on how a Practice configures the Service, we may process: name; email address; the date of birth, phone number and insurance details taken at intake; account information; clinician-assigned plans and exercises; clinician-entered notes; conversation content with the AI companion; direct messages between the client and their Practice, and messages between the client and the clinic their clinician works within, where there is one; appointment and calendar data; mood, theme, and engagement data; exercise/activity data; for physical therapy, workout records (sets, repetitions, hold times, pain and effort ratings, and why a workout stopped), morning check-in answers and questionnaire scores; voice-mode audio that is converted to text to power voice conversations; and reports or exports generated through the platform.

Physical therapy. Where a Practice provides physical therapy, we also process the plan of care the clinician writes or uploads, including the certifying physician's name and National Provider Identifier and the dates of certification (the Service uses AI to read an uploaded plan of care and fill in its fields for the clinician to confirm); exercise videos the clinician uploads, which we store and convert so the Practice's own clients can watch them; and visit notes and the codes and minutes of each visit, where the Practice keeps its notes or bills its visits in Psybird.

Video and voice calls. Where a Practice enables calling, calls connect directly between the participants and are encrypted in transit. We store scheduling and connection metadata (for example, who called whom and when) needed to operate the feature; we do not store call audio or video unless the clinician has Psy take notes from the call, as the next paragraph says.

Session recordings for notes. Where a Practice has Psy take notes in a client's sessions, which needs the client's consent first, a session is recorded on the clinician's device, in person or during a video or voice call. The audio is sent to us (an in-person recording in short pieces while it runs, a call's recording when the call ends), our cloud provider's AI service turns it into a transcript, and Psy drafts a note from the transcript for the clinician to review and sign. We delete the audio once the draft is written; if the AI service is busy, we keep trying for up to 72 hours after the recording ends, then delete the audio and tell the clinician that no note was written. We keep the transcript, so the clinician can check the draft against what was said, until the clinician signs the note, and for no more than 30 days after the recording ends; then we delete it. The draft and the note the clinician signs become part of the Practice's record of care; for a mental health session Psy may also draft the clinician's private psychotherapy notes, which are kept for the clinician alone. A recording is deleted from the device once we have received it, or when the clinician signs out of the device; and if the client's consent was switched off while it was recorded, or the client is no longer with the Practice, it is deleted and no note is written. Session audio and transcripts are not used to train public or third-party AI models.

3.1A Insurance and claims information

Where a Practice turns on insurance billing for a client, we collect and transmit what a standard health care claim requires: the client's name, date of birth, sex and home address; the health plan's name and identifier, the member number and the group number; where the client is covered as someone else's dependent, that subscriber's name, date of birth and relationship to the client; diagnosis codes (ICD-10); procedure codes (CPT or HCPCS) with their modifiers and units; the place and dates of service; and the amount charged. Where a client has a second health plan, we collect the same details for it.

We also receive and store what comes back. A coverage response tells us whether coverage is active, the plan's dates, whether the Practice is in network, and the copay, coinsurance, deductible remaining and out-of-pocket remaining the plan reports. Acknowledgments tell us whether a claim was accepted. Remittance advice tells us what the plan paid, what it adjusted and what it left for the client to pay, and we keep the document the clearinghouse renders for each remittance so the Practice can read it.

If you do not want a service billed to your plan. A client who pays in full out of pocket for a service may ask their Practice not to disclose it to their health plan, and the Practice must agree (45 C.F.R. 164.522(a)(1)(vi)). When the Practice records that request in the platform, we transmit no claim and no coverage inquiry for that client at all.

3.2 Clinician and Practice information

Name; email address; professional and practice information; licensing information when provided; billing and subscription information for the Practice's Psybird subscription (payment card details are collected and processed by our payment processor, Stripe; we do not store card numbers); if the Practice connects its own Stripe account to bill its clients, the business details it enters for that account (legal name, business address, phone, website, and the statement descriptor that appears on its clients' card statements), which

we send to Stripe to open and verify that account; and account and usage information.

Client payments. Where a Practice bills its clients through Psybird, the client saves a card on a page hosted by Stripe, against the Practice's own Stripe account or, where the clinic the Practice belongs to takes its card payments, the clinic's. That page shows the client the authorization the Practice or the clinic asks for, with a link to its financial policy on a page we host, which shows the Practice's or the clinic's name, its policy and its contact and never the client's name; we keep the words the client was shown with the card's record. Psybird never sees or stores card numbers. We store the identifiers Stripe assigns to that saved card, the card brand and last four digits, and a record of each charge and refund (amount, date, and status) as part of the Practice's billing records. To charge a saved card we send Stripe the amount, the currency, a random reference and, so that Stripe can email the client a receipt, the email address Stripe already holds for that card, which the client gave Stripe when saving it and which we read back from Stripe at the time of the charge and do not store. We send nothing else about the client: no name, no session dates, no diagnosis, and no other clinical information. Stripe emails the client a receipt for every charge and every refund, in the name of the Practice or the clinic whose account took the payment. Psybird itself emails clients nothing about money, and a declined charge sends the client nothing automatically. What a client enters on Stripe's own page goes to Stripe under Stripe's own terms.

The claims profile. Where a Practice bills insurance, we also collect what a claim requires about the Practice and the clinician: the clinician's or organization's legal name, National Provider Identifier and NPI type, taxonomy code, license number and state, any Medicare PTAN, the practice address and phone, and the Practice's tax identification number, which for a sole proprietor may be a Social Security number. We send these to the clearinghouse when we register the Practice with a payer and on every claim, because the standard transaction requires them. Where the tax identification number is a Social Security number, it also prints in full on any superbill the Practice produces for a client, which is why the platform asks the clinician to look each one over before it is sent.

Supervision. Where a clinician is pre-licensed and practises under a supervisor, we keep the supervisor's name, credential, license number and state, National Provider Identifier and the dates of the supervision. The Service names the supervisor on the clinician's claims as the supervising provider, prints "Supervised by" with the supervisor's name on superbills, and names the supervisor in the care-management and remote monitoring consents a client is asked for. Where a physical therapist names the assistants who provide care under them, we keep each assistant's name and credential and which lines of a visit an assistant provided, and a superbill names an assistant who provided part of a visit. Psybird does not verify licenses or supervision.

Practice documents. The documents a Practice, or the clinic it belongs to, uploads about the practice, for example its policies, intake paperwork, fee schedule or a clinician's license. We store them and give their text to Psy, which reads it only to answer the Practice's and its clinic's questions, never shares it with a client and never uses it in a client's conversation.

Clinics. Where a clinic uses Psybird, we also keep what the clinic's own account needs: the records of the payouts Stripe makes from the clinic's own Stripe account to its bank (each payout's amount, date and status, and the payments, refunds and fees in it); the lines of any bank statement the clinic uploads to match its deposits (each line's date, amount, a shortened description and any payment trace number in it, and never an account or routing number); the pay rules the clinic sets for its clinicians, what they come to and the pay statement of each pay period; the names and addresses of the clinic's offices; the clinic's conversations with its clinicians and with clients; the clinic's conversations with Psy, with the summaries Psy keeps of their older messages (Section 8); the files its people give Psy, which are kept apart from the clinic's documents, are read by the AI described in Section 7 when given and again only when Psy asks a further question about one, and are read in Psy only for the person who gave them and for the clinic's owners; the spreadsheets Psy makes for them; what Psy remembers for each person and the rules an

owner saves for the whole clinic, which never include anything about a client; and a record of each time someone at the clinic opens a clinician's practice.

People at a clinic. A clinic may give logins to its account to several people: its owners, the members of its staff, and the clinicians it gives clinic access. For a member of a clinic's staff we keep a login (an email address and a password, of which Google holds only a one-way hash) and the clinic's record of them: the name the person who invited them typed, their email address, any words describing their role, the permissions the clinic gave them, whether they are an owner, whether they are invited, active or removed, who invited them and when, when they joined, who removed them and when, their notification choices, their unread counts, the short text of their newest notification, their monthly Psy allowance and how much of it each of Psy's answers used. We do not record when a member of staff was last active. Each person at a clinic sees and does only what the permissions the clinic gave them allow. The clinic's history log records each action a person at the clinic takes that changes something on the clinic's side, downloads such as the list of a month's payments, and each time a person opens a clinician's practice or a client's file in it, and not the pages and lists a person only looks at: when, who and what, and the clinician's practice and the client's record number where the action concerns them, never a client's name or anything the person typed. Only the clinic's owners read it, and it is kept while the clinic exists and deleted with it. Notifications to the people at a clinic appear in the app and in their browser, never by email, and name no client.

3.3 Information collected automatically

When you use the Service or visit our website, we and our service providers may automatically collect technical data such as IP address, device and browser information, log data, and usage information, including through cookies and similar technologies (Section 6). In the context of a health care service, some technical data may be linked to health information and treated accordingly.

4. Sources of information

We collect information: directly from you (for example, when you create an account or use the Service); from the Practice or Clinician that invites and manages a Client, and from the clinic that Practice belongs to, which may enter a new Client's details, book their sessions and file a form the Client signed outside Psybird, and which gives us the name and email address of each person it invites to its account; from another Practice on Psybird, where a Client's record is moved to a new Practice; from our payment processor, Stripe, which tells us the status of a Practice's or a client's payments and saved cards (for example that a card was saved, with its brand and last four digits, or that a payment succeeded or was refunded); from a Client's health plan and from the health care clearinghouse named in Section 10, where a Practice bills insurance, which return coverage responses, claim acknowledgments and remittance advice about that Client's claims; from the federal NPI Registry, when provider details are looked up; from a Client's own request for care sent through psybird.ai/match, when the clinician who replied to it starts the Client's intake from it; and automatically through your use of the Service and website.

5. How we use information

We use information to: provide AI-supported supportive interactions; deliver clinician-assigned exercises; maintain accounts; enable clinicians to review engagement and act on flags; support communication between clients and clinicians, and between a clinic and its clinicians and clients (including secure messaging, scheduling, and video/voice calling); generate reports and exports; support clinical-documentation and Remote Therapeutic Monitoring workflows where applicable; and maintain and improve the security and reliability of the Service.

Consent for sensitive data. Health information, including mental health and physical therapy information, is "sensitive" or "consumer health" data under many laws, which require opt-in consent to collect, use, or share it. Where consent is required, we (and the Practice, as applicable) obtain it before processing (for

clients, through the Client Consent obtained before first use), and you may withdraw consent as described in Sections 12–13. We do not use sensitive data for purposes incompatible with providing the Service.

6. Cookies and tracking technologies

We use cookies and similar technologies to operate the Service, keep you signed in, remember preferences, and understand usage so we can improve reliability and security.

Copies kept in your browser. So that the app opens quickly and keeps working on a poor connection, it keeps a copy of what it last showed you in your browser's own storage on that device: for a clinician, their practice's records, notes included; for a client, their own information; and for a person at a clinic, what the clinic's side of the app last showed them (for example the clinic's home page, the month's billing, the week's calendar and the remote monitoring counts), only what their permissions let them see, for their own login alone, and never what they saw inside a clinician's practice opened from the clinic. The copy holds only what our servers already showed that person and is not sent anywhere. It is deleted when you log out, and when your session is ended from elsewhere, for example when your password is changed or your login is removed; a clinic copy is also deleted when what that person may see at the clinic changes, or their access to the clinic ends. When you open an invitation link to join a practice, or to join a clinic's staff, the app keeps the invitation's key in that browser's storage so that your sign-up can use it, uses it only within 7 days of keeping it, and removes it once it is used; a client's key is never stored in the client's record.

No advertising trackers on health data. We do not place third-party advertising or cross-site tracking technologies (such as advertising pixels) on pages or flows that handle client health information, and we do not use such data for targeted advertising. We honor recognized opt-out preference signals, including Global Privacy Control (GPC), where required.

7. Artificial intelligence and automated processing

The Service uses AI to generate supportive interactions and summaries. AI may encourage reflection, offer emotional support, reinforce clinician-assigned exercises, and support continuity between sessions. For physical therapy, it may also talk a client through their exercises, answer questions about them, and suggest easing off, doing more, or trying a different exercise; those suggestions are general information, not the clinician's instructions. The AI does not diagnose, does not make treatment decisions or change a home program, does not replace a licensed professional, and does not provide emergency services, and its output can be inaccurate. Discuss important concerns or treatment decisions with your clinician.

Where AI processing happens. All AI processing runs through our cloud provider's AI service, under the same Business Associate Agreement with Google that covers the Google Cloud environment that stores platform data; a request may be served from a region outside the United States, and every region is covered by the same agreement. Client content is not sent to any separate AI vendor. Neither Psybird nor Google uses client content submitted through the Service to train generative-AI models.

No training of public AI models on client content. We do not use client conversation content to train public or third-party AI models, consistent with our provider agreements. The AI does not make decisions that produce legal or similarly significant effects about you without a Clinician in the loop.

Psy for a clinic. A clinic's Psy works for each person at the clinic who may use it, within that person's permissions. It may remember what a person asks it to, for that person alone, and the rules an owner saves for the whole clinic, and it refuses to remember anything about a client; read the files the clinic's people give it (our own software turns a spreadsheet into rows first, and Psy may ask the AI a further question about a photo or a scan it has already read); make spreadsheets; read public pages on a fixed list of insurer, government and credentialing websites, itself or through helpers, which are separate calls to the same AI model that are handed a question with no client details, read only pages on that list (our own software turns

a PDF there into text) and return only an answer to the conversation; and run a briefing a person at the clinic set up and approved, on a schedule, with nobody present. A briefing only reads and reports. Nothing Psy prepares changes a record, moves money or sends a message until a person at the clinic taps it, except a repeating reminder a person approved, which is that person's own instruction.

8. Conversation data

To provide continuity, the AI companion uses a limited window of recent conversation as context. That AI-context window is distinct from what the platform stores as the record of care: your Practice's account retains conversation records, summaries, letters, and related data as needed to provide the Service and support your care, subject to the retention practices in Section 14 and to your Practice's own policies. Clinicians may access client conversations when authorized for treatment purposes. Where a clinician's practice is part of a clinic on Psybird, people at the clinic whose permissions allow it can see them as well (Section 9). A clinic's own conversations with Psy are read by the person who had them and by the clinic's owners.

Summaries of long conversations. When a conversation with Psy grows long, or a clinician or a person at a clinic presses Compact in their own, our servers have the same AI model, inside Google Cloud, write a summary of its older messages, which Psy reads in their place from then on. The summary holds what those messages held, is kept with the conversation, may be read by whoever may read that conversation, and is deleted with it; the person still sees every message. A client's messages about harm or a crisis are always kept word for word for Psy. A client's own view of the chat does not change, and their clinician's view of it shows where earlier messages were summarized for Psy.

What Psy keeps to search. When a clinician or a person at a clinic gives Psy a long file, or one of Psy's lookups returns a long result, we keep the whole text on our servers for that conversation so that Psy can search it instead of reading it again. Only that person's Psy, in that conversation, reads it. It expires 24 hours after it was kept and is then deleted, and it is deleted sooner when the conversation is summarized or deleted, and with the Practice or the clinic.

How Psy is put together, and a client's chats. Psy for a client is put together on our servers, each time the client writes, from the client's record as their clinician set it, the summaries of earlier chats, what Psy remembers about the client and the chat so far; the clinician's private notes are never part of it. Psy for a clinician is put together on our servers from what the clinician's device sends with each question. With each question Psy is told the date and time on the Practice's or the client's clock, which is not stored. We store each message a client and Psy exchange, with the time it was said, with the client's record in the Practice's account, beside the summaries their clinician reads, for as long as that record is kept. A client's chat ends by itself after six hours with no new message, as if the client had ended it: its summary and any flag go to the clinician, and what Psy should remember about the client is kept in the client's own record, which the client can read.

9. How we share information

We do not sell your data. We do not sell personal information or consumer health data, and we do not share it for targeted advertising. Any "sale" of consumer health data would require your separate signed authorization, which we do not seek.

We share information only as follows:

- **Treating Clinician / Practice:** client information is shared with the Practice responsible for the client's care, including the reports and exports the Practice downloads, such as a remote monitoring summary a physical therapy Practice gives its own biller. What a Practice does with an export it has downloaded is governed by the Practice's own obligations.

- **The clinic a clinician works within:** where a clinician's practice is a seat in a clinic on Psybird, the people at the clinic can see that practice's records as the permissions the clinic gave them allow, and its owners and the people it allows to see clinical records can see all of them, including client records, notes, conversations with Psy and messages, and those made before the practice joined the clinic, because the clinician directs it by joining. The clinic may move a client's care to another clinician in the clinic, whose practice then receives a copy of the client's record, and keeps a read-only copy of a practice's records when it removes that practice from the clinic (Section 14). A client's messages with the clinic itself are read by the clinic's people; the client's clinician sees them only where the clinic has also given that clinician access to the clinic's side of Psybird. Where Psybird's referral service offers a request for care to a clinician who works within a clinic, the clinic's owners and the people it allows to work its front desk may read and answer it for the clinician (our Consumer Health Data Privacy Policy says more).
- **The client's health plan:** where a Practice bills insurance for a client, the information a claim or a coverage inquiry requires is transmitted to that client's health plan through the clearinghouse named in Section 10, and the plan's responses come back to the Practice. This is the disclosure described in Section 3.1A, and a client can prevent it for a service they pay for in full themselves.
- **Another Practice on Psybird:** where a client's care moves to a different Practice on the platform, the client's record is copied to it. Where the two Practices are not part of the same clinic, the move waits for the client's own authorization.
- **Service providers:** the providers listed in Section 10, under contractual privacy and security obligations and, where they handle PHI, a business associate agreement.
- **Legal and safety:** when required by law, regulation, or legal process, or where necessary to protect the safety, rights, or security of individuals or the Service.
- **Business transfers:** in connection with a merger, acquisition, financing, or sale of assets, subject to this Policy and applicable law.

10. Third-party service providers

We rely on providers to operate the Service. The table below is the current list: what each provider receives, and whether it handles protected health information.

Provider	What it receives	Health information
Google Cloud (Google LLC)	Hosting, database, authentication, serverless functions, file storage (including exercise videos, documents a clinician or a clinic uploads and files given to Psy), logging and monitoring, and the AI models the Service uses, through Firestore, Identity Platform, Cloud Run and Cloud Functions, Cloud Storage, its AI service, and Google's text-to-speech and speech-to-text services. This is where the record of care is stored.	Yes. Under a Business Associate Agreement with Google covering these services.

Provider	What it receives	Health information
Stedi, Inc. (health care clearinghouse)	Only where a Practice bills insurance: eligibility inquiries, claims, claim-status responses and remittance advice. Stedi receives the client's name, date of birth, sex and home address, the health plan's member and group numbers, the subscriber's identity where the client is a dependent, diagnosis and procedure codes, the place and dates of service, the amounts charged, the names and National Provider Identifiers of the clinician who provided the service and of any supervising provider, and the address of the office where it was provided, and, to register a Practice with a payer, the clinician's or organization's name, National Provider Identifier, tax identification number, address and phone.	Yes. Psybird transmits no protected health information through a clearinghouse except under a written agreement meeting HIPAA's requirements for subcontractors.
Stripe, Inc.	Card payment processing, for a Practice's Psybird subscription and, where a Practice turns on client billing, for its clients' payments to the Practice. For client billing the Stripe account belongs to the Practice (or to the clinic that takes card payments for it), client payments settle directly into it, Psybird takes no fee or deduction from them and never receives or holds client funds. To charge a saved card we send the amount, the currency, a random reference and, so that Stripe can email the client a receipt, the email address Stripe already holds for that card, read back from Stripe at the time of the charge; we send nothing else that identifies the client. Stripe emails the client a receipt for every charge and refund. What a client types on Stripe's own page goes to Stripe under Stripe's terms.	No. Billing and payment information only, never client health information.
Cloudflare, Inc.	DNS for our domains, and the network services video and voice calls use: a STUN service that helps two devices find each other, which sees each party's internet address, and, for calls that cannot connect directly, a relay (TURN) that carries encrypted call media it cannot read and does not store; and Turnstile, a check that a request or consultation form on our website is sent by a person, which runs in the visitor's browser and to which we send the visitor's internet address with the check's result.	No. Call media is encrypted between the participants; Cloudflare sees connection data and, on our website, a cookieless count of visits (the page, the referring page, the country and device type); never what you write to us.
Google Workspace	Operational and notification email. A notification is written to carry no clinical detail. The exception is an appointment: a session reminder, or notice that an appointment was scheduled or changed, states its date and time.	Limited, as described, and under Google's Business Associate Agreement.
Apple and Google push-notification services	The short text shown as a notification on a phone, with that device's notification token. An appointment notice or a session reminder states the date and time of the session. An incoming call shows the name of the practice on the client's screen, and the name of the client on the clinician's, so each knows who is calling.	Limited, as described. These services deliver the notification and receive nothing else.

Provider	What it receives	Health information
National Library of Medicine (PubMed) (U.S. National Institutes of Health)	Search terms, when a clinician asks the assistant to look up published research, or when a question a physical therapy client asks Psy calls for it, in which case only the topic is sent, never the client's own words. The Service blocks and does not send any search containing a name from the Practice's roster, a date, an email address, a phone number, or a run of five or more digits.	No. No client information is sent.
Insurer, government and credentialing websites (a fixed list)	The address of a public page, when someone at a clinic asks Psy to research a payer's or an agency's rules, or a briefing the clinic set up does, and Psy reads that page. Nothing about a client is sent, and the Service refuses a request that would carry a client's name, date of birth, member number or other information about a client.	No. No client information is sent.
NPI Registry (Centers for Medicare and Medicaid Services)	A provider's National Provider Identifier, or a provider's name and state, when provider details are looked up. A public federal registry.	No. Provider information only.

Loading our website or app also contacts the services that deliver its fonts and code libraries, Google's reCAPTCHA Enterprise, which checks that a visitor is not automated (on our website's request and consultation forms Cloudflare Turnstile does the same), and, on a phone, Apple's App Attest or Google's Play Integrity; Google Crashlytics receives a report from the mobile apps if one crashes. These receive technical data such as an internet address, a browser or device description and, for a crash, what the app was doing when it stopped. They receive no health information and no account content. Psybird's in-browser read-aloud voice, which is switched off in the current release, downloads its voice files from huggingface.co when it is on; that download carries nothing about the person using it.

A provider that handles protected health information does so under a business associate agreement and is limited to using the information as needed to provide services to us. We keep a written inventory of our providers, and we do not send protected health information to a provider before the agreement covering it is in place. This list is current as of the date of this document, and we update it here when it changes.

11. HIPAA and protected health information

Where we provide services to a Practice that is a HIPAA covered entity or business associate, and PHI is involved, we act as a business associate under a BAA and maintain administrative, technical, and physical safeguards designed to protect PHI, including authentication, access controls, encryption in transit and at rest, logging, and incident-response procedures. Our infrastructure and AI processing run on Google Cloud under an executed Business Associate Agreement with Google. For PHI, your rights under HIPAA (such as access and amendment) are generally exercised through your healthcare provider, whose HIPAA Notice of Privacy Practices describes them.

12. Washington consumer health data (My Health My Data Act)

If you are a Washington resident, or your consumer health data is collected in Washington, the Washington My Health My Data Act may give you additional rights regarding health data that is not covered by HIPAA. These include the right to confirm whether we collect, share, or sell your consumer health data; to access it; to have it deleted; to withdraw consent; and to obtain a list of the third parties and affiliates with whom it has been shared. We do not sell consumer health data, and we do not operate geofences around healthcare

facilities to identify, track, or message individuals.

Separate policy. These rights, and the categories, sources, purposes, and recipients of consumer health data, are described in our separate Consumer Health Data Privacy Policy, linked distinctly from our homepage as required by MHMDA. To exercise MHMDA rights, use the contact method there or in Section 19.

13. Your privacy rights and choices

Depending on where you live, you may have rights under state privacy laws (for example, California's CCPA/CPRA and the Virginia-model laws now in effect in roughly twenty states). Whether a given law applies depends on the law's thresholds and your residence. These rights may include:

Right	What it means
Access / know	Confirm whether we process your data and request a copy and details about our processing.
Delete	Request deletion of your personal data, subject to legal exceptions (note MHMDA's deletion right is broader).
Correct	Request correction of inaccurate data.
Portability	Receive certain data in a portable, commonly used format.
Opt out of sale / sharing / targeted advertising	We do not sell or share personal data for these purposes; we honor Global Privacy Control where required.
Limit / withdraw consent for sensitive data	Limit use of sensitive personal information or withdraw previously given consent.
Non-discrimination & appeal	We will not discriminate against you for exercising your rights, and (where the law provides) you may appeal a denied request.

How to exercise your rights. Contact us using Section 19. We will verify your request as required, allow use of an authorized agent where permitted, and respond within the timeframe the applicable law requires (generally within 45 days). For PHI, please contact your healthcare provider, as HIPAA rights are exercised through them.

14. Data retention and deletion

We retain personal information only as long as needed to provide the Service, support care and documentation workflows, comply with legal obligations, resolve disputes, and maintain security. Retention of PHI is governed by the BAA and the Practice's instructions; client records are generally retained for the duration of the care relationship and then handled as the Practice directs. When a Practice ends its use of the Service, we make client records available for export and delete our copies within 30 days, with backups purged on our rolling cycle (daily backups retained 14 days, plus a point-in-time recovery window), except as this section says. When a Practice's account is deleted, or a client leaves a Practice, we keep for that client a copy of what they could see in the app (their file, their messages and their conversations with Psy), which only they can open, until they delete their own login. When a Practice removes a client, we keep that copy and the client's login only until the client downloads the copy, or for 30 days, and then delete both. We keep a record of each move of a client's care between Practices (the two Practices, the clinicians' names, the client's first name and the dates) and the note the sending clinician wrote for the receiving one, as our record of the move. We keep the record of each agreement a person accepted in the Service (their email address and name, the documents and their version, and when) after their account is deleted, as evidence of that agreement. Messages sent through our website's contact and consultation forms, and problem

reports sent to us, are kept until we delete them; you can ask us to delete yours (Section 19). Where a clinic removes a clinician's practice from the clinic, the read-only copy of that practice's records kept for the clinic is retained until the clinic's account is deleted: the clinic is offered a download of it first, and it is deleted with the account. A clinic's history log, its records of its people and what Psy remembers for its people are kept while the clinic's account exists; before the owner who created the account deletes it, they are offered the clinic's export, which includes them, and they are deleted with it. A summary of a conversation's older messages is kept with the conversation and deleted with it, a client's stored chats with Psy are kept as long as the client's record, and the text kept for Psy to search in a conversation expires 24 hours after it was kept and is then deleted (Section 8). An export a clinician or a clinic asks for is assembled on our servers and kept there for seven days so that it can be downloaded, and then deleted. Where we close a Practice's or a clinic's account ourselves, it stays closed for 30 days, during which its owner can download its records, and is then deleted (Terms of Service, Section 16). When a Practice's or a clinic's account is deleted, in any way, we keep our own record of each invoice we raised to it (the month, the amounts, the status and the payment processor's reference for it), which holds nothing about its clients, as part of our billing records. Operational logs and our cloud provider's access logs are kept for 30 days, our own audit records of access to health information for at least 6 years, and billing records for 7 years. You may contact us for information about applicable retention periods; our internal Data Retention & Disposal Schedule governs the details.

15. Data security and breach notification

We use administrative, technical, and organizational safeguards designed to protect information, including authentication, permission-based and restricted access, encryption in transit and at rest, secure infrastructure providers, audit logging, and monitoring and incident-response procedures. No method of electronic storage or transmission is completely secure.

What our own staff see. Psybird's operators work from an internal app. It shows each account's own business details, its billing, how much each client's use of Psy cost in calls and in the amount of AI processing (never the words), outcome totals with the number of clients behind each figure, and bug reports. A client's email address is shown hidden: showing it in full needs a reason, lasts five minutes and is logged, with the reason, where the client's Practice can read it. The name, email address and words of a request for care sent through psybird.ai/match are shown only after a reason is given, which is logged. Suspending or closing an account, undoing a closure and pausing Psy each need a reason, which is written to a log only our operators read. When a client reports a reply from Psy as harmful, we email Psybird's owner which practice it came from and when, and never the words of the conversation.

Breach notification. If a breach affecting your information occurs, we will provide notifications as required by applicable law, which may include HIPAA's Breach Notification Rule (via the affected Practice), the FTC's Health Breach Notification Rule, and state breach-notification laws. Our procedures are described in our internal Breach Response Plan.

16. Children's privacy

The Service is intended for use under the direction of a licensed professional. Accounts are not available to children under 13, and we do not knowingly collect personal information from children under 13. A client aged 13 to 17 may use the Service only with a mental health Practice, only where permitted by law and with the documented consent of a parent or legal guardian, obtained and verified by the supervising Practice consistent with applicable minor-consent laws. A client of a physical therapy Practice must be an adult: at least 18 years old and at least the age of majority where they live.

17. International users

The Service is intended for use in the United States. Your information is stored in the United States (our primary data storage is in a U.S. Google Cloud region); some processing, including the AI features, may take place in other regions of the same provider, under the same HIPAA Business Associate Agreement with Google. If you access the Service from outside the United States, you do so on your own initiative and are responsible for compliance with local law.

18. Changes to this Privacy Policy

We may update this Policy from time to time. We will post the updated Policy with a new effective date and, for material changes, provide reasonable notice (for example, by email or in-app notice). For new categories of health data or new purposes, we will obtain any consent required by law before the change takes effect.

19. Contact us

Psybird.ai (operated by Any Percent LLC)

Privacy contact / to exercise your rights: Yani Chris Tsoukalas, Founder

Email: support@psybird.ai

Address: 1135 Scott Ave, Bremerton, WA 98310