

Privacy Policy

Effective October 6, 2026 · Version 2026-10-06

Underline.AI, Inc., a Delaware corporation ("Underline," "we," "our," or "us"), operates the **Underline.Health** platform. This Privacy Policy explains how we collect, use, and protect personal data belonging to **visitors to our website and to the clinicians and staff who hold accounts** with us.

What this policy does not cover

This policy **does not** govern the patient records that clinicians place in the Services. Those records are processed only on the instructing clinician's behalf and are governed exclusively by the data protection agreement applicable to that clinician's region:

- United States: the [Business Associate Agreement](#), under HIPAA
- Israel: the [Israeli Data Protection Addendum](#), under the Protection of Privacy Law, 5741-1981

Where this policy and one of those agreements differ with respect to patient records, that agreement governs. **Patients do not hold accounts with Underline, do not log in, and never interact with the Services.** We have no direct relationship with any patient and do not contact them.

1. Definitions

- **Clinician** — a licensed mental health professional or practice that holds an account with us. In the United States a Clinician is a Covered Entity or acts on behalf of one; in Israel a Clinician is the owner and controller of the database.

- **Authorized User** — a colleague, supervisee, or staff member to whom a Clinician grants access within their workspace.
- **Personal Data** — information that identifies or can reasonably be linked to an identified or identifiable individual.
- **Patient Records** — the clinical content a Clinician places in the Services concerning the individuals they treat. Patient Records are outside the scope of this policy, as described above.

2. Personal Data we collect

a. Information you give us. When you create an account or contact us, we collect your name, email address, practice or clinic name, professional details, time zone, and billing contact information.

b. Payment information. Payments are processed by our payment processor. We receive confirmation of a transaction, a subscription status, and limited billing metadata. We do not receive or store full payment card numbers.

c. Information collected automatically. When you use our website or the Services we collect device and browser type, IP address, language settings, pages viewed, feature usage events, session duration, and similar diagnostic and analytics data.

d. Security and audit information. We record authentication events and administrative actions taken within your workspace, including the acting user and the time. These records exist to protect your account and to satisfy our security obligations.

e. Marketing information. If you submit an enquiry or sign up for updates, we collect the information you provide and how you reached us, including campaign parameters.

We do not ask for, and you should not send us, patient information through our website, support enquiries, or marketing forms.

3. How we use Personal Data

We use Personal Data to provide, operate, secure, and support the Services; to authenticate you and protect your account; to process payments and manage subscriptions; to communicate with you about your account, security, and material changes; to understand and improve how the Services are used; and to meet our legal and regulatory obligations.

We do not sell Personal Data, and we do not use Personal Data or Patient Records for advertising.

We do not use your content or Patient Records to train, fine-tune, or improve generative AI models, and we contractually prohibit our AI subprocessors from doing so.

4. Legal bases for processing

Where the EU or UK General Data Protection Regulation applies, we rely on: performance of a contract with you; our legitimate interests in securing, operating, and improving the Services, where not overridden by your rights; compliance with legal obligations; and, where required, your consent, which you may withdraw at any time.

Where Israeli law applies, we process Personal Data on the basis of your consent given when you open an account and in accordance with the Protection of Privacy Law, 5741-1981.

5. Sharing and subprocessors

We share Personal Data with service providers who help us operate the Services, including cloud infrastructure, transcription and AI model providers, email delivery, payment processing, and product analytics. Each is bound by contract to process data only on our instructions and to protect it appropriately. Our current subprocessors are listed at <https://underline.health/subprocessors/>.

Processing by AI providers. The Services use third-party AI to create transcripts, draft clinical documents, answer questions in Guide, and read photographed notes.

To provide these features, we send the content you place in the Services to the following providers, and only to them:

- **Amazon Web Services**, through Amazon Bedrock, which runs Anthropic's Claude models. It receives the session information, notes, transcripts and photographed notes needed to draft documents and answer questions. Anthropic does not receive your data; Amazon Web Services is the processing party.
- **Deepgram, OpenAI** and Amazon Transcribe (part of Amazon Web Services), which receive recording audio for transcription and return the transcript. None of them receives any other clinical record.

These providers process the content only to return the result to us, are bound by business associate or equivalent data protection agreements, may not retain it beyond processing, and may not use it to train or improve their models. Where that content includes Patient Records, it is processed under the data protection agreement for your region described above. Our mobile apps ask for your permission before any of your content is sent to these providers.

We may also disclose Personal Data where required by law or valid legal process, to protect our rights or the safety of any person, or in connection with a merger, acquisition, or sale of assets, in which case we will give notice before your data becomes subject to a different privacy policy.

6. International transfers

We operate on infrastructure located in the United States. If you access the Services from Israel, the European Economic Area, or the United Kingdom, your Personal Data will be transferred to and processed in the United States. Where such a transfer is subject to the GDPR, we rely on the European Commission's Standard Contractual Clauses or another lawful transfer mechanism. Transfers of Personal Data out of Israel are made in accordance with the Protection of Privacy Regulations (Transfer of Data Abroad), 5761-2001.

If your workspace is in Israel, the transfer of **Patient Records** to the United States, and the safeguards that apply to it, are addressed in Section 5 of the [Israeli Data](#)

[Protection Addendum](#) rather than in this policy.

7. Retention

We retain account Personal Data for as long as your account is active and for as long afterwards as is necessary to meet our legal, tax, and regulatory obligations or to resolve disputes. Security and audit records are retained for six years. Retention and deletion of Patient Records is governed by the data protection agreement applicable to your region, not by this policy.

8. Your rights

Depending on where you are located, you may have the right to access the Personal Data we hold about you, to correct it, to delete it, to restrict or object to its processing, to receive it in a portable format, to withdraw consent, and to lodge a complaint with your supervisory authority — in Israel, the Privacy Protection Authority; in the EEA or UK, your national data protection authority.

To exercise any of these rights, contact privacy@underline.health. We will respond within the period required by applicable law.

Requests concerning **patient** rights — access, amendment, or an accounting of disclosures — must be directed to the treating Clinician, not to us. As a processor acting on the Clinician's behalf we will support the Clinician in responding, as set out in the applicable data protection agreement.

9. Account deletion

You may request deletion of your account and its associated data by writing to privacy@underline.health, or from within the mobile app, following the instructions at <https://underline.health/delete-account/>. Because clinical records are subject to retention obligations that fall on the Clinician rather than on us, we will confirm the scope and timing of deletion with the account holder before acting, and we will

return or destroy Patient Records in accordance with the applicable data protection agreement.

10. Cookies and analytics

We use cookies and similar technologies for authentication, security, preferences, and product analytics. You can refuse or delete cookies through your browser settings, though some features may not function correctly as a result. Our analytics are configured to record product usage events and account identifiers only; they are not configured to capture the content of clinical records.

11. Security

We apply administrative, physical, and technical safeguards appropriate to the sensitivity of the data we hold, including encryption of data in transit and at rest, verified database connections, least-privilege access controls, multi-factor authentication, tamper-evident audit logging, and continuous monitoring. Further detail is published at <https://underline.health/security/>. No system is perfectly secure, and we cannot guarantee absolute security.

12. Children

The Services are provided to licensed professionals and are not directed to children. We do not knowingly collect Personal Data from children through our website or account registration. Clinical records concerning minors may exist within a Clinician's workspace; the lawful basis for creating and holding those records, including any parental or guardian consent, is the responsibility of the treating Clinician.

13. Changes to this policy

We may update this policy. We will notify account holders of material changes by email or within the Services before they take effect. Continued use after the

effective date constitutes acceptance.

14. Contact

Questions, requests, or complaints may be sent to privacy@underline.health.

Underline.AI, Inc. privacy@underline.health <https://underline.health>