

Israeli Data Protection Addendum

Effective August 6, 2026 · Version 2026-08-06 · Applies to Israeli workspaces

This Israeli Data Protection Addendum (this "Addendum") supplements and is incorporated into the [Terms of Use](#) between **Underline.AI, Inc.**, a Delaware corporation ("Underline," "we," or "us"), and the clinician, clinic, or entity accepting it (the "Clinician" or "you").

This Addendum applies to workspaces in Israel and is the Israeli counterpart to our Business Associate Agreement. HIPAA does not apply to your practice, and no Business Associate Agreement is offered for an Israeli workspace. Where a document elsewhere in our terms refers to a "data protection agreement," this Addendum is that agreement for you.

You accept this Addendum when you create your workspace.

1. Framework and roles

1.1 Applicable law. This Addendum is framed by reference to the Protection of Privacy Law, 5741-1981 (the "PPL"), including Amendment 13 thereto, and the Protection of Privacy Regulations (Data Security), 5777-2017 (the "Data Security Regulations").

1.2 Roles. You are the **owner** and **controller** of the database comprising your patient records, and you determine the purposes and means of their processing. Underline is a **holder** and processor, processing those records solely on your documented instructions and on your behalf. Underline does not determine the purposes of processing and has no independent right to the records.

1.3 Security classification. The parties acknowledge that a database containing mental health information is treated as subject to the **high security level** under the Data Security Regulations, and Underline will apply controls consistent with that classification.

1.4 Scope. This Addendum governs **patient records** — the clinical content you place in the Services concerning the individuals you treat. Personal data concerning **you** as an account holder is governed by the [Privacy Policy](#).

2. Processing

2.1 Instructions. Underline will process patient records only as necessary to provide the Services, as set out in this Addendum, or as required by applicable law. If Underline is required by law to process records otherwise, it will inform you before doing so unless the law prohibits that notice.

2.2 Purpose limitation. Underline will not use patient records for its own purposes, will not sell them, and will not use them for marketing or advertising.

2.3 No training of models. Underline will not use patient records, and will not permit any subprocessor to use them, to train, fine-tune, or otherwise improve any generative artificial intelligence model.

2.4 Data minimisation. Underline will process only the records necessary to provide the Services, consistent with the data minimisation principle reflected in the PPL and the Data Security Regulations.

2.5 Anonymisation. Underline may anonymise patient records so that the resulting information can no longer be attributed to an identifiable individual, whether directly or indirectly, taking into account all means reasonably likely to be available for re-identification. Anonymised information is not patient records and falls outside the scope of this Addendum. Underline may use anonymised information to operate, secure, evaluate, and improve the Services and to produce aggregate statistics. Underline will not attempt to re-identify anonymised information, will not contact any patient, and will not use anonymised information to train, fine-tune, or otherwise improve any generative artificial intelligence model.

2.6 Your responsibilities. You are responsible for the lawful basis on which you collect and hold patient records, including obtaining any consent required under section 1 of the PPL; for providing patients any notice required of you; for the accuracy of the records; for your own retention obligations under Ministry of Health guidance and professional regulation; and for registering your database with the Registrar of Databases where registration is required.

2.7 Confidentiality. Underline will ensure that personnel authorised to process patient records are bound by confidentiality obligations and are appropriately trained.

3. Security measures

3.1 Standard. Underline will implement and maintain organisational, physical, and technical security measures appropriate to a high security level database under the Data Security Regulations.

3.2 Current measures. These presently include: encryption of records in transit using TLS 1.2 or higher and at rest under customer-managed keys for the primary database and its snapshots; verification of database server certificates against a pinned certificate authority; role-based access control on a least-privilege basis with no long-lived static credentials; multi-factor authentication for administrative access; administrative access only through session-recorded channels, with no inbound shell access to production systems; tamper-evident, append-only logging of access to records, retained for six years; object-level logging of reads and writes on the clinical asset store; automatic deletion of session audio following transcription; and point-in-time recovery of the database.

3.3 Access records. Underline maintains automated records of access to patient records, consistent with regulation 10 of the Data Security Regulations, and will make relevant extracts available to you on reasonable request.

3.4 Review. Underline reviews its security measures periodically and following any material change to its systems or to the risks it faces.

4. Subprocessors

4.1 Authorisation. You authorise Underline to engage subprocessors to process patient records. A current list is published at <https://underline.health/subprocessors/>.

4.2 Flow-down. Underline will impose on each subprocessor, by written contract, data protection obligations no less protective than those in this Addendum, and remains fully responsible to you for each subprocessor's performance.

4.3 Changes. Underline will give at least thirty (30) days' notice before a new subprocessor begins processing patient records. If you reasonably object on data protection grounds, you may terminate the Services without penalty and receive a pro-rata refund of prepaid fees.

4.4 Urgent substitution. Where a subprocessor must be replaced urgently to preserve the security, integrity, or continuity of the Services — including on a subprocessor's service failure, security incident, or withdrawal of service — Underline may make the change without advance notice and will notify you promptly afterwards, stating the reason. The written flow-down required by Section 4.2 must be in place before the replacement processes any patient records, and your objection and termination rights under Section 4.3 apply equally to a change made on this basis.

5. Cross-border transfer

5.1 Location. Patient records are processed on infrastructure located in the **United States**. By accepting this Addendum you acknowledge and instruct that transfer.

5.2 Basis. The transfer is made in accordance with the Protection of Privacy Regulations (Transfer of Data Abroad), 5761-2001, on the basis that Underline undertakes by this Addendum to comply with the conditions for holding and using the data that apply to a database in Israel, including the confidentiality, security, purpose limitation, and data subject rights obligations set out here, and will not transfer the data onward except to a subprocessor bound by equivalent obligations under Section 4.

6. Security incidents

6.1 Notification to you. Underline will notify you **without unreasonable delay and no later than twenty-four (24) hours** after becoming aware of a severe security incident affecting your patient records, and will provide a complete report **no later than thirty (30) calendar days** after becoming aware, containing what is known about the nature of the incident, the records affected, the individuals affected, the measures taken to contain and mitigate it, and the measures taken to prevent recurrence.

6.2 Your regulatory obligations. As the database owner, you are responsible for notifying the Privacy Protection Authority of a severe security event as required by regulation 11(d) of the Data Security Regulations, and for notifying data subjects if the Authority so directs. **That obligation is immediate.** The notification period in Section 6.1 is an outer limit and not a waiting period: Underline will notify you as soon as it is practicable to do so, and will provide the information you reasonably need to make your own notification without delay, including before its own investigation is complete.

6.3 Cooperation. Underline will cooperate with you and with the Privacy Protection Authority in the investigation of any incident and will not make a public statement identifying you without your prior written consent unless required by law.

6.4 Routine unsuccessful events. Underline's systems are subject to frequent unsuccessful attempts at unauthorised access — scans, probes, denied connections, and failed log-on attempts — that do not result in access to patient records. This Section constitutes notice of those events, and no individual notice of them is required.

7. Data subject rights

7.1 Requests to you. A data subject's right of review under section 13 of the PPL, and the right to request correction under section 14, are exercised against you as the database owner.

7.2 Assistance. Underline will provide you with reasonable assistance, taking into account the nature of the processing, in responding to such requests. The Services allow you to retrieve, correct, and export records directly at any time.

7.3 Requests received directly. If Underline receives a request from a data subject concerning your patient records, it will not respond substantively and will forward the request to you within five (5) business days.

8. Audit

Underline will make available to you the information reasonably necessary to demonstrate compliance with this Addendum, including a description of its security measures and, where available, third-party assessments. Where you reasonably require further assurance, the parties will agree a proportionate approach that does not compromise the confidentiality or security of other customers' data.

9. Term, return, and deletion

9.1 Term. This Addendum takes effect when you accept it and continues for as long as Underline holds your patient records.

9.2 Export. You may export your records through the Services at any time, and for thirty (30) days following termination.

9.3 Return or deletion. Following that export period, Underline will delete or return all patient records, including those held by subprocessors, and retain no copies, **within sixty (60) days**. Underline will confirm completion in writing on request. Requests should be sent to legal@underline.health.

9.4 Retained copies. Where deletion is not immediately possible because records persist in immutable backup media, Underline will continue to apply the protections of this Addendum to those records until the backups expire on their ordinary schedule, will keep them encrypted and access-controlled, and will not restore them to production use.

9.5 Your retention obligations. Deletion by Underline does not discharge your own obligation to retain medical records for the period required by Israeli law and professional regulation. You are responsible for exporting and retaining records before requesting deletion.

10. General

10.1 Conflict. In the event of a conflict between this Addendum and the Terms of Use with respect to patient records, this Addendum governs.

10.2 Amendment. Underline may amend this Addendum where required by law or regulation on thirty (30) days' notice; any other amendment requires your acceptance.

10.3 Governing law. The Terms of Use are governed by the laws of the State of Delaware. Nothing in this Addendum or in that choice of law limits the application of the PPL and the Data Security Regulations to your database, or your rights or the rights of data subjects under Israeli law.

10.4 Notices. Notices to Underline under this Addendum must be sent to legal@underline.health and are effective on receipt.

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