# Privacy Notice for Healthcare Provider - Recorded Conversations

**Effective Date:** June 2026

## 1. Purpose of This Notice

You are receiving this notice because you have agreed to participate in a recorded conversation with a representative of STEM's client (the "Client') that may be uploaded to [STEM's AI Recording tool] (the "App") for the purpose of analysis. We are committed to protecting your privacy and complying with data protection legislation including the General Data Protection Regulation (GDPR). The application is designed as a coaching and insight generation tool, and not as a compliance monitoring, surveillance, or audit system.

This Privacy Notice applies globally. Additional jurisdiction-specific privacy information, including any local rights or requirements, may apply depending on your location and is set out in the relevant country-specific annex to this Notice. If there is any difference between this Privacy Notice and a country-specific annex, the annex will apply to ensure compliance with local law.

## 2. Who Is Responsible for Your Data

Data Controller: STEM Healthcare Ltd
Contact Email: quality@stemhealthcare.com
Postal Address: First Floor, The Waterman, 151 Farringdon Road, London, England EC1R 3DE
Data Protection Officer (DPO): privacy@inizio.com

## 3. What Data We Collect

We will collect and process the following personal data:
- Audio recording of your conversation.
- Metadata such as the date, time, and duration of the recording.

We do not intentionally collect any special category data (e.g., health, political opinions) unless it is voluntarily disclosed during the conversation. Audio files are processed to remove personally identifiable information and are subsequently anonymized so that individuals cannot reasonably be identified.

## 4. Legal Basis for Processing

Your data is processed based on your consent under Article 6(1)(a) of the GDPR. You may withdraw your consent at any time by contacting us at the email address above. Where anonymized data is used for analytical or service improvement purposes, such data is no longer personal data under applicable data protection laws.

## 5. How Your Data Will Be Used

The recording may be:
- Uploaded to STEM's AI tool for analysis to gain actionable insights, service improvement and

coaching purposes. Personal data is not used to train or fine-tune STEM's AI tool, and any ongoing use is based only on anonymized or aggregated data.
- Deleted from the user's device without being uploaded to the app, within [e.g., 7 days].
- Processed to extract aggregated and non-directive insights relating to communication patterns, interaction quality, and engagement dynamics for the purpose of analysis and service improvement and coaching. measures such as response timing, frequency, and interaction flow to assess how actively a participant engages, verbal cues that reflect the depth and coherence of the participant's contributions, the style and intensity of communication without attributing emotional or psychological states, analyze speech patterns and interaction dynamics to infer engagement levels, without profiling psychological states of participants, and to improve service quality
- Deleted after analysis is complete, within [e.g., 30 days].
Sales representatives do not have access to the content of the recordings and are only able to upload audio files securely via the mobile app.

Your data will not be used for marketing or shared with third parties for unrelated purposes.

Outputs generated are standardized and anonymized and are not intended to identify individuals or be used for monitoring or evaluation of specific persons. STEM AI is not designed to act as a repository of recordings or as a system for retrospective review of individual interactions.

## 6. Data Sharing and Transfers

Your data may be processed by trusted third-party service providers (e.g., cloud storage or analytics platforms) under strict confidentiality and data protection agreements. If data is transferred outside the EEA, we will ensure appropriate safeguards are in place. Personal data is not shared for the purpose of independent third-party analysis or model training.

## 7. Data Security

We apply appropriate technical and organizational measures to protect your data from unauthorized access, loss, or misuse. All audio recordings are secured throughout their lifecycle on the app and associated directly with the user that records them by associating the user's unique identifier with the recording when it is uploaded. All audio recordings are encrypted at rest using a device specific encryption key stored on the device's secure key storage rendering, preventing the user or a malicious actor with direct memory access from viewing the recordings. All audio recordings are encrypted in transit. Once a recording has been successfully uploaded, it is immediately deleted from the user's device to ensure we do not retain any (albeit encrypted) recordings for longer than required. STEM does not combine datasets in a manner intended to re-identify individuals.

## 8. Data Retention

We will only retain your personal data for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting, tax, reporting requirements or as is consented to by yourself. Recordings are retained for a limited period (typically up to 90 days) and are deleted after processing. Non-anonymized data is deleted as soon as analysis is complete.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We will anonymize your data so that it can no longer be associated with you, after which it may be used for statistical analysis, service improvement, coaching and research purposes on an aggregated basis.

## 9. Your Rights

Under GDPR, you have the right to:
- Access your personal data.
- Request correction or deletion.
- Withdraw your consent at any time.
- Lodge a complaint with a supervisory authority.

To exercise your rights, please contact us at quality@stemhealthcare.com.

In relation to any deletion request, we ask you to note that where your personal data remains identifiable, it can be deleted. However, as recordings are anonymized during processing, there is typically no remaining personal data to delete once processing is complete.

## 10. Contact

If you have any questions about this notice or how your data is handled, please contact:
STEM Healthcare Ltd
Email: quality@stemhealthcare.com
Phone: +44 (0) 20 3861 3999
DPO: Group Data Protection Officer

## Annex 1 – Jurisdiction-Specific Information

This Annex provides additional information for individuals located in specific jurisdictions. Where there is any inconsistency between this Annex and the main Privacy Notice, this Annex will take precedence for individuals in the relevant jurisdiction.

**United Kingdom**

- Applicable Law: UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Supervisory Authority: Information Commissioner's Office (ICO) – www.ico.org.uk
- Right to Lodge a Complaint: You have the right to lodge a complaint with the Information Commissioner's Office (ICO) if you believe your data protection rights have been infringed. The ICO can be contacted at: www.ico.org.uk
- Internal Complaints Process: We encourage you to contact us in the first instance so that we can investigate and attempt to resolve your concern. Complaints relating to how your personal data is handled can be submitted to: Email: quality@stemhealthcare.com. We will acknowledge and investigate complaints in line with our internal data protection complaints handling procedure.

**Portugal**

- Supervisory Authority: Comissão Nacional de Proteção de Dados (CNPD) – www.cnpd.pt
- You have the right to lodge a complaint with the CNPD.
- Information provided in this Notice is intended to be clear and accessible in accordance with Portuguese transparency requirements.

**Brazil**

- Applicable Law: Lei Geral de Proteção de Dados (LGPD)
- You have the right to confirm processing, access data, request anonymisation, blocking or deletion, and request information about data sharing.
- Processing is based on your consent under Article 7, I LGPD. You may withdraw consent at any time.
- Data Protection Officer (Encarregado): Esperanza Avila.

**Mexico**

- Applicable Law: Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)
- Supervisory Authority: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) – www.gob.mx/buengobierno
- Individuals have the right to exercise ARCO rights (Access, Rectification, Cancellation, and Opposition) in accordance with applicable law.
- Privacy notices must be made available in Spanish and include clear information on processing purposes and data transfers.

- Specific consent requirements apply to data transfers unless an exemption under law is met.

**Canada**

- Applicable Law: Personal Information Protection and Electronic Documents Act (PIPEDA); in Quebec, Act respecting the protection of personal information in the private sector (Law 25)
- Processing is based on meaningful consent, which must be clear, informed, and given for specific purposes.
- In Quebec, privacy notices must be made available in French (unless otherwise requested).

**Spain**

- Supervisory Authority: Agencia Española de Protección de Datos (AEPD) – www.aepd.es
- You also have rights under Spanish data protection law (LOPDGDD), including digital privacy rights.
- A summary version of this notice may be provided where required.

**Germany**

- Applicable Law: General Data Protection Regulation (GDPR) and Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG)
- The application is not used for employee monitoring, profiling, or performance evaluation.
- Processing is based on explicit consent.
- You may lodge a complaint with the competent German supervisory authority.

**Italy**

- Supervisory Authority: Garante per la Protezione dei Dati Personali – www.garanteprivacy.it
- Processing follows principles of necessity, proportionality, and minimisation.

**South Korea**

- Applicable Law: Personal Information Protection Act (PIPA)
- Separate consent is obtained for recording, analysis, and cross-border transfers.
- Personal data is destroyed without delay once the purpose is achieved.
- Audio files are permanently deleted using secure deletion methods.

**Japan**

- Applicable Law: Act on the Protection of Personal Information (APPI).
- Personal data is used only within specified purposes.
- Information on cross-border transfers is available upon request.

**France**

- Supervisory Authority: CNIL – www.cnil.fr
- No individual profiling or behavioural scoring is carried out.
- Analysis is limited to aggregated insights.
- Only necessary data is processed.

**China**

- Applicable Law: Personal Information Protection Law (PIPL)
- Separate consent is obtained for recording, AI analysis, and cross-border transfers.
- You will be informed of overseas recipients, purpose, and safeguards.
- You have the right to request explanation of automated processing.