Saltdean and Rottingdean Medical Practice

Privacy Notice: Use of Heidi Health AI Scribe

Last updated: March 2026

About This Notice

This supplementary privacy notice explains how Saltdean and Rottingdean Medical Practice uses patient data when using Heidi Health, an AI-powered medical scribe, during consultations. It should be read alongside our main practice privacy notice.

What is Heidi Health?

Heidi Health is an AI-powered scribe that listens to conversations during your consultation and produces a draft of the clinical notes. It uses speech recognition and natural language processing to transcribe the discussion and generate structured documentation.

Heidi is purely a note-taking tool. There is no element of the AI influencing or advising the clinician's thinking or decision-making. It does not make clinical decisions, suggest diagnoses, or recommend treatments.

All notes generated by Heidi are reviewed, edited if necessary, and approved by your clinician before being saved to your medical record. The clinician retains full responsibility for all documentation entered into your record.

Purpose of Processing

The use of Heidi Health aims to:

- Allow clinicians to focus on you during the consultation rather than on typing notes
- Improve accuracy and completeness of medical record-keeping
- Reduce administrative workload for clinicians
- Support the generation of letters, referrals and other clinical documentation

Categories of Data Processed

The following types of personal data may be processed when Heidi is used during a consultation:

- Name and other identifying details discussed during the consultation
- Date of birth, address, contact details
- Medical history, diagnoses, symptoms and examination findings
- Medications, prescriptions and allergies
- Test and investigation results
- Family and social history
- Sexual orientation, gender identity or relationship status (where discussed)
- Clinician information, including their voice and professional identifiers

Legal Basis for Processing

The legal bases for processing your personal data under the UK GDPR and the Data Protection Act 2018 are:

Article 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 9(2)(h) – Processing is necessary for the provision of health or social care or treatment, or the management of health or social care systems and services.

In addition, verbal consent is obtained from each patient before the AI scribe is activated. While consent is not relied upon as the sole lawful basis for processing (as clinical records cannot be deleted simply because consent is withdrawn), it provides an important additional transparency and control mechanism for patients.

How Your Data is Processed

During a consultation where Heidi is used, the following process takes place:

1. Your clinician explains that Heidi will be used and asks for your verbal consent.

2. If you consent, the clinician activates the recording. Heidi captures the audio of the conversation.

3. The audio is transcribed into text. The audio recording is automatically deleted once transcription is complete and is not stored.

4. Identifiable information within the transcript undergoes de-identification and pseudonymisation, where personal identifiers are removed or replaced with coded references.

5. The pseudonymised transcript is processed by the AI model to generate structured clinical notes.

6. The clinician reviews the generated notes, makes any corrections, and approves them.

7. The approved notes are then copied into your medical record in SystmOne. The clinician re-identifies the record at this stage to ensure accuracy.

Data Controller and Processor

Data Controller: Saltdean and Rottingdean Medical Practice (sole controller)

Data Processor: Heidi Health (Tier 1 Trading Pty Ltd), 49 Greek Street, London, W1D 4EG

A Data Processing Agreement is in place between the practice and Heidi Health. Heidi Health also has data processing agreements with its sub-processors, including Amazon Web Services UK (cloud hosting) and Google LLC (processing within the EU/Ireland).

Data Security

Heidi Health employs the following security measures:

- End-to-end encryption of data in transit and at rest
- ISO 27001, Cyber Essentials, and SOC 2 certifications
- Regular security audits, penetration testing, and real-time monitoring
- Compliance with NHS Data Security and Protection Toolkit (DSPT) standards
- Compliance with the Digital Technology Assessment Criteria (DTAC)
- Role-based access control (RBAC), applying the principle of least privilege
- UK-based data hosting on Amazon Web Services UK servers

No patient-identifiable data is shared with third parties. Access to pseudonymised data by Heidi staff is only permitted for troubleshooting purposes, with the express permission of the clinician.

Data Retention

Audio recordings are automatically deleted once transcription is complete and are not stored.

Transcripts and generated clinical notes within the Heidi platform are subject to auto-deletion. The practice has configured this to a 1-day retention period, after which data is automatically and irreversibly deleted from Heidi's systems.

Once the clinician has approved and saved the notes into SystmOne, they form part of your medical record and are retained in accordance with the NHS Records Management Code of Practice. No identifiable data is retained by Heidi Health after the auto-deletion period.

International Data Transfers

All data is processed within the UK or Ireland (EU). Some sub-processors, such as Google LLC, process data within the EU (Ireland), which is covered by an adequacy decision. No data is transferred outside of the UK and EU.

Your Rights

Under data protection law, in relation to Heidi Health you have the right to:

- Object to the use of Heidi during your consultation – simply inform your clinician before or during the appointment
- Request access to your consultation records by contacting the practice
- Request correction of any inaccuracies in your health records
- Request details of how your data is processed by Heidi
- Raise a complaint about data handling with the practice, our DPO, or the ICO

Contact

For questions about this notice, about how your data is processed by Heidi Health, or to withdraw consent for future use, please contact the practice.

Caldicott Guardian: Dr Jason Bolton, GP Partner

Data Protection Officer: Laura Taw, Senior IG Consultant and DPO, NHS South, Central and West

ICO: ico.org.uk/make-a-complaint | 0303 123 1113

A Data Protection Impact Assessment for this processing has been completed and is available on request.