Data Protection Impact Assessment (DPIA) for Heidi AI Use Case (Real-Time Consultation Transcription)

Controller: [Marston Forest Healthcare]

Date of DPIA: [02/04/25]

Description of Processing Activity:
Heidi AI is used as a transcription tool by some clinicians at MFH to transcribe live clinician-patient consultations in real time. This tool listens to the conversation between the clinician and patient, generating consultation notes based on that interaction. Explicit patient consent is obtained before each session, informing patients of how their data will be processed and used.

1. Purpose and Scope of the DPIA

This DPIA assesses the data protection and privacy implications of using Heidi AI to capture real-time clinician-patient interactions for transcription. The scope includes assessing GDPR compliance, obtaining patient consent, and managing data securely within NHS standards.

2. Nature of Data Processed

- **Data Type**: Spoken interactions between clinician and patient, which may contain patient-identifiable information (PII), such as names, health conditions, treatments, and other personal information relevant to the consultation.
- **Data Sensitivity**: High, as this is identifiable patient health information.

3. Processing Basis and Lawful Grounds

The lawful basis under UK GDPR for processing patient information in this way is:

- *Article 6(1)(e)* (necessary for the performance of a task carried out in the public interest)
- *Article 9(2)(h)* (for the provision of healthcare and treatment management).

As this involves recording identifiable data from patient interactions, **explicit patient consent** is required under *Article 6(1)(a)*, which allows for processing based on the individual's consent.

4. Consent Process

- **Consent Requirement**: Patients are fully informed of the purpose, scope, and nature of the recording, with clear explanations about data usage and retention.
- **Documentation**: Consent is documented before each session, either via digital signature, verbal confirmation recorded in the patient record, or a signed consent form.
- **Withdrawal**: Patients are informed they may withdraw consent at any time, and this will stop the recording immediately.
- **Privacy Notice:** Information relation to the use of Heidi must be included on the practice Privacy Notice which is available on the practice web site.

5. Data Collection and Minimisation

- **Data Collection**: Real-time recording of patient-clinician interactions with the minimum necessary information captured for accurate clinical documentation.

- **Minimisation**: Only relevant clinical information is recorded, ensuring that personal and sensitive data beyond the scope of medical care is avoided where possible.

6. Data Security

- Heidi AI adheres to NHS Digital standards for data protection and encryption.
- **Access Control**: Only the clinician has access to the transcriptions during the session, and the transcriptions are securely stored in accordance with GDPR and NHS requirements.

7. Risk Assessment

Risk	Likelihood	Impact	Mitigation
Recording sensitive patient interactions without consent	Low	High	Explicit consent is required and documented prior to recording each session
Data breach or unauthorized access	Medium	High	NHS-approved security protocols and encryption ensure data protection and controlled access
Inaccurate transcription	Medium	Medium	Clinician reviews all transcriptions for accuracy before entry into the patient's medical record

8. Data Retention and Disposal

Heidi AI is configured to delete recordings after **1 day**, which is the minimum automated retention period permitted within the app. If shorter retention is required, manual deletion is available. After clinician review, relevant notes are entered into the Electronic Health Record (EHR) system, with any remaining data removed according to Heidi AI's 1-day retention setting or manually deleted as needed.

9. Rights of the Data Subjects

Patients are informed of their rights to access, rectify, and object to the use of their data under GDPR. They are also informed of their right to withdraw consent at any time during the consultation. If consent is withdrawn, recording ceases, and any data captured is promptly deleted.

10. Mitigation Actions

1. **Ongoing Monitoring**: Regularly review Heidi AI's compliance status and updates to NHS and GDPR guidelines.
2. **Staff Training**: Ensure clinicians and staff are trained on obtaining consent and securely handling patient data.
3. **Routine Audits**: Conduct periodic audits to verify that consent documentation and data deletion protocols are strictly followed.

11. Approval

DPIA Completed by: Dr Ismail
Date: 02/04/25
Data Protection Officer (if applicable): Paul Couldrey