Cambridge Private Doctors (CPD Health Ltd.) Practice Privacy Notice (PPN)

– **Contact details of the practice as data controller:**

Dr Yvonne Girgis-Hanna, Cambridge Private Doctors, Nuffield Health Hospital, 4 Trumpington Street, Cambridge
enquiries@cambridgeprivatedoctors.co.uk

– **Contact details for the data protection officer**

Dr Yvonne Girgis-Hanna, Cambridge Private Doctors, Nuffield Health Hospital, 4 Trumpington Street, Cambridge
enquiries@cambridgeprivatedoctors.co.uk

– The purposes for processing the data and the legal basis for processing the data –

Processing is for direct patient care in accordance with the Health and Social Care Act 2012 Articles 6(1)(e) and 9(2)(h)

– other legal bases when processing for reasons other than direct care include a direction under the Health and Social Care Act 2012 – where disclosures are a legal requirement the lawful basis and special category condition for such processing are: '…for compliance with a legal obligation…' (Article 6(1)(c)) and Article 9(2)(h) '…management of health or social care systems…';
– for medical research the lawful basis and special category condition are Article 6(1) (e) '…for the performance of a task carried out in the public interest…'

In the face of an objection from a patient, in many cases we would be likely to be able to demonstrate 'compelling legitimate grounds' for continued processing for the safe provision of direct care and processing which is necessary for compliance with a legal obligation.

We rely on legitimate interests as the lawful basis for processing patient data.
CPD has applied the three-part test to demonstrate that we have fully considered and protected individual's rights and interests.

The three-part test as applied to CPD

Purpose – the provision of medical care
Necessity – without processing data, we cannot provide safe medical services to the patient
Balance – We respect the interests & fundamental rights, and freedoms of our patients, which require the protection of personal data

– **Information about with whom data are shared:**

We hold demographics about our patients (name, date of birth, email)
We keep clinical records of consultations with patients
This information is kept solely for the provision of medical care for our patients. It is strictly personal between us and the patients. Any communication with outside agencies will usually be with secondary care medical services as an integral part of medical care provision to the patient.

Our medical records are kept securely on UK servers. In addition, a secure copy of medical records is also kept for patients that we see at the Nuffield Hospital. This is to ensure that if you are being treated as a patient at the Nuffield, a full copy of your medical records is available to your medical practitioner. Without your express permission, these records will not be released to any other third party.**– Our patients have the right to access their medical records and to have inaccurate data corrected**

Our patients have a right to see the entire contents of their medical records at no cost.
Requests should be made in writing rather than verbally.
We reserve the right to remove any information specifically relating to a third party, such as a separate letter with confidential information about another patient.
In this situation, the patient asking for release of all records will be notified of any omissions

We will reply within one month
We reserve the right to refuse or charge for manifestly unfounded requests
or excessive.
If we refuse a request, we will tell the individual why and that
In case of conflict you have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

– **Retention periods**

– Our GP records are retained until the death of the patient or request to delete data by the patient

- **Complaints**

– Our patients are entitled to lodge complaints with the Information Commissioner's Office (ICO). If they feel that their rights have been breached

- **Consent**

We do not ask for formal consent from patients for using an electronic medical record (this is stated clearly to all patients on booking appointments. Similarly, we do not formally ask for permission to share clinical information (usually when we refer - at the patient's request- to another specialist). Information is kept solely for the provision of medical care for our patients. It is strictly personal between us and the patients. Any communication with outside agencies will usually be with secondary care medical services as an integral part of providing medical care to the patient.

This is in line with the official guidance.

> Explicit consent under the GDPR is distinct from implied consent for sharing for direct care purposes under the common law duty of confidentiality.
>
> The GDPR creates a lawful basis for processing special category health data for the provision of direct care that does not require explicit consent.
> A common example of implied consent is when a patient agrees to a referral from one healthcare professional to another. In these circumstances, the patient's agreement implies their consent to share relevant information to support the referral (unless the patient objects).

The only exception to the above would be where there is a legal requirement to disclose, such as a direction under the Health and Social Care Act 2012 or disclosures under public health legislation.

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

Controller: CPD Health Ltd

Date of DPIA: 04/01/2025

Description of Processing Activity:
Heidi Al is used as a transcription tool by CPD 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.

1. Purpose and Scope of the DPIA
This DPIA assesses the data protection and privacy implications of using Heidi Al 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 (P), 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
Under the UK GDPR, the lawful basis 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) and 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 and given clear explanations about data usage and retention.
• Withdrawal: Patients are informed they may withdraw consent at any time, and this will stop the recording immediately.

5. Retention
The recordings are permanently deleted one week after the transcription