Pimlico Osteopathy

CLINIC DATA PROTECTION PROCEDURE

V0 – 5/5/2018
V1 – 16/5/2018
V2 – 17/5/2018

Appointed person with responsibility for data protection	**DUNCAN WEBSTER**
Registered with the Information Commissioners Office	DUNCAN WEBSTER

Clinic Data Protection Policy

Information Held

The following information is collected: Patient name, address, date of birth, email address, phone numbers, GP details, past medical history, family medical history and case history for treatment carried out at clinic.

All information is given by the patient or their carer, parent or legal guardian.

Data Collection

Information collected is sufficient for the purpose of making informed clinical decisions.

Data is collected verbally on the phone by reception staff or practitioners to book appointments and take contact details. Medical information is collected by osteopaths verbally at a face to face appointment. From time to time, medical information may also be discussed over the phone at the patient's discretion.

Patient contact details, appointments and clinical records are stored electronically.

Older patient details are stored on paper, and these are gradually being moved to digital storage or destroyed.

Data Storage

Electronic records are stored on an external booking system, www.cliniko.com. The servers are physically based in Australia, but we have signed a Data Processing Addendum with them confirming that they will adhere to all GDPR legislation, including for any of their subprocessors. For more information on their infrastructure and their GDPR compliance, you can read here. In particular, their server security details are here.

Current paper records are stored onsite in a lockable cabinet, and only certain practitioners have key access.

In the event of the death of the holder of the patient records, the other practitioners will still be able to access the notes, either digitally or via the locked box.

Data disposal (minimum 8 years, 25 years of age for children)

Records cannot be deleted before statutory requirements for data retention – 8 years or up to 25 years of age for children.

Pimlico Osteopathy

Paper notes are archived after **5 years. They are then securely stored at** 68 Fairfield Road, East Grinstead, West Sussex. RH19 4HB.

Notes are destroyed by **shredding/incineration** after **8 years or 25 years of age for children.**

Electronic records are deleted from the system after **8 years or 25 years of age for children.**

Consent

Patient data is also used for **appointment reminder text messages and emails**, a **newsletter and marketing** which patients opt in to with a **tick box online** or **verbally on their first visit**. We check patients still want to receive communications on **a regular basis**.

We process your data using the lawful basis of **consent for marketing, and fulfilment of contract and legitimate interest** for processing your medical record and **sending you health information and exercises** relating to your condition. Your medical record is processed as Special Category Data under Article 9 2(h) of the GDPR.

Parents must give consent for communication with children under 16 years.

Data Sharing

Information is only shared with other persons with patient's permission. This would usually be with other health professionals. Patient information is never passed on to external practitioners, persons or companies.

Data would extremely rarely be shared without consent if there was a legal order or in cases of serious safety risks.

Data Checks

Every **year** we perform checks on **5%** of our patient's data records to make sure they are accurate.

Whenever a patient arrives after an absence of more than a year, we will recheck their data.

Security

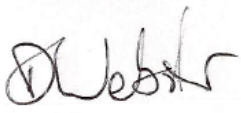
Access to paper records is restricted to **practitioners and admin staff** who have signed a **confidentiality agreement.**

All electronic data is password protected at a server level and **access to information can be restricted by user role. Practitioners systems are kept updated and antivirus security systems are in place and updated.**

Passwords are changed **every 6 months (December 31st, June 30th).**

Data breaches will be detected by observing signs of unauthorized entry to storage areas, monitoring communications or becoming aware of a security breach (e.g. a virus or unauthorized log on or change to permissions) on the computer system. Data breaches will be investigated and reported to the Information Commissioner's Office within 72 hours by the appointed person. Patient's will be informed if we believe a data breach has occurred.

Patients may contact the Information Commissioner's Office if they believe a data breach has occurred. Information Commissioner's Office: 0303 123 1113
Subject Access Requests
All staff know that subject access requests must be responded to within a month and no charge can be made. Data is only released on receipt of a signed request from patients or in exceptional circumstances. Any data sharing is detailed in the patient record.
Patient Rights
Patient's and anyone we hold data about have some rights under GDPR: You can request to: see your data at any time, move your data to another practice, correct any inaccuracies, prevent marketing. You may request for details to be deleted but due to our legal obligation we cannot delete your health record. However, **we can and will remove you from our contact list**.
Complaints
Patients or staff may raise any complaints about data processing with our Data Controller who may be contacted at: **duncan@pimlicoosteopathy.com** or on **07880542823** You may also contact the Information Commissioner's Office Directly on: 0303 123 1113

Name:	Duncan Webster	Signature:	
Position:	**Principal**	Practice:	**Pimlico Osteopathy**
Date:	5th May 2018	Review Date:	4th May 2019

This signature is the practice signing implementation of the policy.