

CLINIC DATA PROTECTION PROCEDURE

This is a starting template but you will need to significantly modify this for your practice. Please delete as appropriate and add or remove information for your own clinic policy. You may wish to share this document or a modified version to fulfil your duty to inform your patients how you process their data. Remember you may also process data for employees and you will need to share your procedure with them and give them data protection rights.

This is not just a form to complete, it is a policy that your practice must be following to comply with the law.

Appointed person with responsibility for data protection

Robert David

Registered with the Information Commissioners Office

Fully Registered

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. We may also take details on lifestyle and social circumstances and employment and education details.

Data Collection

Information collected is sufficient for the purpose of making informed clinical decisions. These can also include

Data is collected verbally on the phone by Robert David to book appointments and take contact details. Medical information is collected by the Osteopath verbally at a face to face appointment.

Patient contact details and appointments are stored on the computer. Patient clinical records are held manually.

Data Storage

Consultation Data is stored manually in a locked filing cabinet.

Some clerical data is held electronically. These can be held by Robert David on a password-protected apple mac and a password-protected iCloud. Some GDPR-compliant third parties also hold some data, such as Acuity scheduling

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

All notes are held in house in a locked filing cabinet. Only Robert David has the key to the cabinet

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**, a **newsletter and marketing** which patients opt in to **with a tick box/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 sold or passed on to other practitioners, persons or companies without permission.

To run the practice and provide a clinic service we use the following **third parties**:

123 reg: <https://www.123-reg.co.uk/terms/privacy.shtml>

Skype: <https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx>

Vodafone: https://www.vodafone.com/business/media/document/gdpr_slideshare.pdf

Facebook: <https://www.facebook.com/business/gdpr>

Twitter: <https://twitter.com/en/privacy>

Acuity Scheduling: <https://acuityscheduling.com/privacy.php>

Square: <https://squareup.com/gb/legal/privacy>

Quickbooks: <https://quickbooks.intuit.com/uk/gdpr/>

Google mail: <https://cloud.google.com/security/gdpr/>

Weebly: <https://www.weebly.com/uk/privacy>

[yell.com](https://www.yell.com)

Sometimes we refer patients to and from other medical professionals using written letters or (rarely) emails or text messages. These companies may have access to some of your details. We are confident that these companies are all following data protection regulations.

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

Data Checks

Patients records are checked for accuracy through conversation within the clinic consultation, and updated where necessary.

Security

Only Robert David has direct access to the electronic and manual records.

All electronic data is password protected and antivirus is updated within the apple system

Passwords are changed on an annual basis.

Data breaches will be detected by observing signs of unauthorised entry to storage areas, monitoring communications or becoming aware of a security breach (e.g. a virus or unauthorised 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 Robert David. 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

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 but we can remove you from our contact list.

Complaints

Patients or staff may raise any complaints about data processing with our Data Controller (Robert David) who may be contacted at: 07842131671

You may also contact the Information Commissioner's Office Directly on: 0303 123 1113

Name:	Robert David	Signature:	ROBERT DAVID
Position:	Osteopath / Data Controller	Practice:	Highlight Osteopaths
Date:	23 May 2018	Review Date:	23 May 2020

This signature is the practice signing implementation of the policy.