Otley Osteopath's data protection and privacy policy

Background

- General Data Protection Regulation (GDPR) – enforcement date 25th May 2018
- Most recent update 26th May 2020
- Applies to all companies processing and holding data in EU
- Data includes; customers, employees, suppliers
- Personal Data is any info related to a person that can be used directly/indirectly to identify a person (name, photo, email, bank, social media post, medical info)
- Regular data processing is the collecting, storing and use of personal data
- Data Processor – processes info on behalf of a controller
- Data Controller – defines purpose, conditions and use of personal data.
- Fine for serious breaches

Personal data collected, used and stored by Otley Osteopaths (OO)

*mobile device – phone, iPad, laptop

- Employees past and present – CV's (paper), Insurance (paper and mobile devices), GOSC details (paper), Bank details (online banking – password protected), Personal Data (paper), contact details (paper and mobile devices), social media contacts (mobile devices). All paperwork for employees is stored in a locked filing system, all electronic data is password protected.
- Patients – (paper, booking system online)
    - Patient notes – paper, mobile devices
        - Data stored includes – contact details, personal details, sensitive medical details (as required for the service offered by OO and regulated by GOSC), GP details
        - Paper notes stored in clinic premises in locked cabinet
        - Locked cabinet code only known by Osteopaths to access patient paper notes which contain sensitive medical data when required. Notes filed immediately and privacy and confidentiality maintained at all times. Cabinet locked if Osteopath leaves the room.
        - Patients' personal, medical and health information may also be stored within our electronic data processing system. Any system used by OO will be required to meet GDPR requirements and we also will require that any party holding information is registered with the Information Commissioner's Office (ico.).
        - Only persons making bookings, bookkeeping or administrating for OO will have access to the data stored in the booking system.

- Only registered osteopaths representing OO have access to medical notes and information about your health.
- If medical notes need to be printed and transported (for the facilitation of home visits or corporate visits) then they will be kept in a container which will remain on the person of the osteopath at all times until returned to the locked filing system or shredded (only shredded if an electronic copy is kept).
- Professional medical letters (names, GP, medical info) stored on password protected database. (Two lines of security – device code, database password)
- Patient lists (first names and surname) may be printed daily and held by osteopath and reception team to facilitate running of clinic. Collected at end of clinic, filed in locked filing cabinet.
- Receipts with personal details on are handed over in person or emailed using only an email address confirmed by the patient. Any copies of such documents will be filed away in locked cabinets.

  - Booking system – mobile devices
    - Contact details – telephone, email, name
    - Accessible by mobile devices – which are password protected: Reception personnel (for booking appointments and taking payments), Osteopaths (for booking appointments and running clinics), Director (for monitoring clinic availability) and Bookkeeper (for bookkeeping)
    - Current booking system is 'Cliniko', who facilitate for full GDPR compliance and are registered with the ICO.
    - Cliniko uses emails and text messages to confirm and remind patients of appointments. The emails are sent to the patient and clinic facility only. There are no mailing lists used for marketing unless specifically agreed to by patients.
    - To increase security, any holder of one of our Clinko accounts must have a password protected mobile device. The system automatically times out any session if left inactive.

- Suppliers – Contact details of previous suppliers (stationary, equipment, clinic room rent) who's details are widely available online.

The data we obtain is stored and is only used to facilitate further patient bookings or treatments. We do not share or distribute information to any other party. We use contact detail information to contact patients only for the purpose of providing due care as regulated by the General Osteopathic Council. We do not use contact information for advertising purposes unless specifically agreed to by our patients.

Our employee and contractors data is stored to provide professional certification as required by the Osteopathy governing body. Data is not used or processed any further than this.

Consent

- Must be given in intelligible and easily accessible format. With the purpose for data processing attached to that consent. Language must be plain and clear. It must be as easy to withdraw consent as to give it. Parental consent must also be given in less than 16 years old.
- Our stored data comes directly from a patient, contractor or employee. There is no 3rd party data.
- Patients are asked for their contact details when booking their initial appointment. We explain that their details are stored on our booking system but are kept confidential. If people give their details this is therefore implied consent. They also give specific consent to be contacted via phone or email on their initial appointment. This form is then signed by the patient or completed via link sent only to their email address. *During the coronavirus pandemic, and electronic form sent via an email link is deemed sufficient consent.*
- On the initial appointment patients are given a medical consent form to sign which explicitly and clearly explains that we store their medical details for 8 years (or until a child's 25th birthday) confidentially in order to provide their treatments and is seen only by Osteopaths. Only Osteopaths have access to the sensitive medical details.
- Sensitive medical information is only shared (verbally or written) with other medical professionals with explicit informed consent from the patient. This is a key part of professional confidentiality. Letters are posted to a named person or given directly to the patient themselves to hand to their Doctor in a sealed envelope.
- Our non-sensitive data is processed only by osteopaths, directors, receptionist, bookkeepers and managers of Otley Osteopaths in order to manage clinic requirements using patient statistics. This data is not distributed in any way.
- Employee and contractors data (contact details, contracts and professional data) is stored in a locked filing system and kept confidential. The only people with access to this are the directors and managers of OO.
- Social Media – any social media posts that have quotes from patients have been anonymised and explicit consent gained that their quote is to be put on a social media site.
- Children (under 16 Years) are required to have parental countersignature to give consent for treatment and therefore storage of their medical information.

Privacy by design

- Data should be held and processed as absolutely necessary for the completion of duties (data minimisation). Access to data should be limited to those needing to act.
- OO limits patient sensitive data to the osteopaths involved in their care only. Contact data is stored only for use when booking patients in. It is not processed or distributed any further.
- Medical notes are stored for 8 years (if adult) or until a child's 25th birthday as per the Osteopathic regulating body (GOSC) guidance.

Right to be forgotten / data Erasure

That the data controller should erase their personal data when

a) The data is no longer relevant to the original purposes of processing

b) Data subject withdraws consent

For OO patient medical data is stored for 8 years (or until child's 25th birthday) in line with recommendations from the Osteopathy governing body. Should the subject request that their contact details are removed from the booking system this will be carried out immediately, however their medical records are stored as per legal requirements.

For OO employee data this is stored for 5 years after they have finished working with OO, the data is then confidentially deleted or destroyed.

The method of data deletion is confidential shredding for paper documents and deletion of data stored on electronic devices.

Security

- Our patient records are stored in a number code locked filing system within the clinic. Only Osteopaths that are providing treatments to the patients know the code. Notes are filed immediately after use and are not visible to other patients.
- The booking software that is used has a password security feature. Osteopaths, directors, bookkeepers and reception personnel have access to the booking software. There is no sensitive medical data accessible to anyone else than OO osteopaths through the software.

Subject Access Rights

- Right for data subjects to obtain whether information on them is being processed, where and for what purpose. If requested the controller shall provide a copy of personal data free of charge in electronic format.
- The right to access all personal data, on request from the subject, will be completed within 1 month.

Data Protection Officer

Only required if the company is

a) Public authority

b) Does large scale systemic monitoring

c) Large scale processing of sensitive data

As OO does not meet any of these specifications a data protection office is not required.

Data Breach

- A data breach for OO would consist of medical notes or the booking software being compromised.
- Serious breaches must be reported to the Information Commissioners Office, within 24-72 hours. Serious breaches are those which risk the rights and freedoms of individuals (discrimination, financial loss, loss of confidentiality). This is not likely for OO given the data we hold on patients.
- OO staff are trained as to what constitutes a data breach and are required to inform a director immediately. The Director will then manage the data breach.