The Derbyshire Sporting Joint

Data Protection Policy, including Key Procedures

Date: April 2018
For review: April 2020

1. Aims of this Policy

The Derbyshire Sporting Joint needs to keep certain information, including personal data, on its employees, associates, work experience students and clients to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the EU General Data Protection Regulation (GDPR) which comes into effect on 25 May 2018. To comply with the law, personal information will be collected and used for specified, explicit and legitimate purposes, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This policy applies to employed and associate clinical and administrative staff. This document also highlights key data protection procedures within the organisation.

2. Definitions

Personal data is any information related to a person, or **data subject,** that can be used to directly or indirectly identify the person. Examples include: name, photo, email address, bank details and medical information.

A data **controller** is the organisation that determines the purposes, conditions and means of the processing of personal data. A data **processor** is an organisation that processes personal data on behalf of a data controller.

Processing data is defined as obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

Consent to processing personal data must be explicit; the request for consent must be clear, easily accessible and separate from consent to treatment. Consent must be as easy to withdraw as to give. Parental consent is required to process the personal data of children under 16.

3. Types of information processed

The Derbyshire Sporting Joint processes personal information to enable us to provide services to our clients, to maintain our accounts and records, promote our services and to support and manage our associate staff and employees.

The Derbyshire Sporting Joint processes personal data that may include the following:

a. Client contact information, date of birth, medical history, family details, lifestyle and social circumstances, registered GP, treatment notes, referral letters to and from other healthcare providers, reports from scans and investigations, and communications with insurance companies.
b. Employee and associate contact information, next of kin, employment and education details, bank account and payroll information, supervision and professional review notes.
c. Contact information relating to healthcare practitioners, suppliers, business contacts and professional advisers.

Personal information is kept in the following formats:

a. Paper records.

b. Electronic records held on computer, cloud storage service, web-based practice management software, online clinic booking system and insurance company web-based systems or portals.

4. Notification

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner https://ico.org.uk. We notify and renew our notification on an annual basis as the law requires.

In case of any interim changes, these are notified to the Information Commissioner within 28 days. The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is **Miss Kate Stalker.**

5. Responsibilities

Administrative and clinical staff process personal data within The Derbyshire Sporting Joint. Personal data is shared with insurance companies and other healthcare practitioners as appropriate and in line with legal obligations. Where personal data is processed by third parties written contracts exist between The Derbyshire Sporting Joint and the third party processor to ensure compliance with the GDPR.

In line with the GDPR principles, The Derbyshire Sporting Joint will strive to ensure that personal data collected is:

a. obtained fairly and lawfully
b. obtained for a specific and lawful purpose
c. adequate, relevant and not excessive
d. accurate and kept up to date
e. not held longer than necessary, in line with current legislation
f. processed in accordance with the rights of data subjects
g. subject to appropriate security measures
h. not transferred outside the European Economic Area (EEA)

Where necessary or required we may share personal data with individuals (data subjects) themselves and other agencies, for example:

- other healthcare professionals
- social and welfare organisations
- family, associates and representatives of the data subject
- suppliers and service providers;
- financial organisations
- current, past and prospective employers;
- employment agencies and examining bodies

Where this is necessary we are required to comply with all aspects of the GDPR. All employed and associate staff who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in disciplinary proceedings.

6. Policy Implementation

To meet our responsibilities, our procedures will ensure the following:

a. Any personal data is collected in a fair and lawful way
b. It is clearly explained why the personal data is needed at the start
c. Only the minimum amount of personal data needed is collected and used
d. The personal data used is up to date and accurate

e. Personal data is kept safely
f. The length of time personal data is held is reviewed and managed through a retention and destruction schedule
g. The rights people have in relation to their personal data can be exercised
h. Everyone managing and handling personal information is trained to do so
i. Anyone wanting to make enquiries about handling personal data, whether a member of staff or someone using our services, knows what to do
j. Any disclosure of personal data will be in line with our procedures
k. Queries about handling personal data will be dealt with swiftly and politely, in compliance with the GDPR.

7. Training

Training and awareness raising about the GDPR and how it is followed will take the following forms:

a. On induction, staff will be asked to read this policy and clinic guidelines, and sign to confirm they have read and understood the information:

b. Awareness raising: Data protection issues will be discussed at regular staff meetings and an information notice displayed in the staff room.

8. Gathering and checking information

Before personal information is collected, we will consider what details are necessary for our purposes and ensure that at least one of the lawful bases for processing personal data apply. These are:

a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
b) Contract: the processing is necessary for a contract we have with the individual, such as credit card payment details.
c) Legal obligation: the processing is necessary for us to comply with the law regarding maintenance of healthcare and employment records.
d) Vital interests: the processing is necessary to protect someone's life.
e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party.

We explain to clients on the Patient Details Form, which they complete before receiving our services, why we need specific pieces of personal information and what the information is used for. Personal sensitive information will not be used apart from the exact purpose for which permission was given. No third parties have access to information apart from those that they give consent to.

9. Data Security

The organisation will take steps to ensure that personal data is always kept secure against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Patient records are held by the therapist during the treatment session and then placed in the office for filing. The office is kept locked when unoccupied.

- Patient records are stored in a lockable filing cabinet, in a locked room. Archived records are stored separately for seven years and are then destroyed.

- Computer systems are password protected and equipped with up to date anti-virus software. When the reception desk is left unattended for short lengths of time, the electronic diary has a privacy option to maintain confidentiality and prevent unauthorised access.

- Patient records may be shared electronically via secure email and through insurance company web-based portals.

- The clinic is always staffed, and when not open to clients, is locked securely.

- Patient records are not removed from the clinic.

- Some data is processed on behalf of the clinic by third parties, such as payroll services and the practice management software system. The clinic has written contracts of data processing with all third parties so as to ensure the safe management of data and compliance with the GDPR.

Any unauthorised disclosure of personal data to a third party by a member of staff will result in disciplinary proceedings.

10. Retention Schedule

Patient records are retained for seven years after the last date of attendance at the clinic and are then destroyed.

Personal data relating to previous employees and associate staff is kept for six years and PAYE data is retained for three full tax years from the date of them leaving employment at the clinic and is then destroyed.

Personal data relating to prospective employees and associate staff is destroyed after six months following completion of the relevant recruitment process.

11. Subject Access Requests

Under the GDPR provides people have the right to

a. obtain confirmation that their data is being processed
b. access their personal data and supplementary information.

This right of access allows individuals to be aware of and verify the lawfulness of the processing. Miss Kate Stalker is responsible for ensuring the subject access request is responded to in a timely way.

Fees

We will provide a copy of the information **free of charge**. If the request is obviously unfounded or excessive, particularly if it is repetitive, we will charge a 'reasonable fee' as allowed by the GDPR. This is calculated in relation to the administrative cost of providing the information.

We may also charge a reasonable fee to comply with requests for further copies of the same information.

Timeframe for response

Information will be provided without delay and at the latest within one month of receipt of the subject access request.

Where requests are complex or numerous, we may extend this by a further two months. We will inform the person making the request of this within one month of receipt and explain why the extension is necessary.

Unfounded or excessive requests

We may

a. charge a reasonable fee

b. refuse to respond, explaining why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy within one month.

Providing the Information

a. We will verify the identity of the person making the request, using 'reasonable means'.

b. If the request is made electronically, we will provide the information in a commonly used electronic format.

c. Where we hold a large quantity of information about an individual, we will ask the individual to specify the information the request relates to.

Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If we have disclosed the personal data in question to others, we will contact each recipient and inform them of the rectification (unless this proves impossible or involves disproportionate effort). If asked to, we will also inform the individual about these recipients.

We will rectify the data within one month, or three months where the request for rectification is complex. If we do not take action in response to a request for rectification we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

Right to Erasure

Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

a. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
b. When the individual withdraws consent.
c. When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
d. The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
e. The personal data must be erased in order to comply with a legal obligation.

There are some specific circumstances where the right to erasure does not apply:

Where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- archiving purposes in the public interest, scientific research historical research or statistical purposes
- the exercise or defence of legal claims.

If we have disclosed the personal data in question to others, we will contact each recipient and inform them of the erasure (unless this proves impossible or involves disproportionate effort). If asked to, we will also inform the individual about these recipients.

It is noted here that in the case of providing healthcare services there is usually a legal obligation to maintain patient records for a stipulated timeframe and this legal obligation would be a justifiable reason not to erase the personal data.

Other requests

Under the GDPR, there are several other requests individuals can make including to restrict or object to processing. In all cases we will respond in line with the requirements of the GDPR, Articles 18 to 23.

12. Documentation

Under Article 30 of the GDPR we are required to document certain information regarding our data processing activities including categories of data we process, security measures and controller-processor contracts. This documentation is reviewed regularly and kept up to date.

13. Managing Data Breaches

A data breach is an accidental or unlawful disclosure, alteration, loss or destruction of personal data held by the clinic. It affects the confidentiality, integrity or availability of personal data. This may be due to human error, equipment failure, unforeseen damage such as fire, or malicious acts such as a computer virus.

All personal data breaches will be recorded

- In the case of a personal data breach we will establish (with reference to Recital 85 of the GDPR) the likelihood and severity of the resulting risk to people's rights and freedoms, meaning the potential negative consequences.

- If it's likely that there will be a risk then we will notify the ICO; if the risk is low, we will make sure the reason for not informing the ICO is clearly documented.

- We will report a notifiable breach to the ICO not later than 72 hours after becoming aware of it.

    - a description of the nature of the personal data breach including, where possible:

    - the categories and approximate number of individuals concerned; and

    - the categories and approximate number of personal data records concerned;

    - a description of the likely consequences of the breach, and the measures taken to deal with it and mitigate any possible adverse effects.

- If a breach is likely to result in a substantial risk to the rights and freedoms of individuals, we will inform those concerned directly as soon as possible.

- We will describe the nature of the breach and:

    - the name and contact details of the liaison person within the clinic

    - a description of the likely consequences of the personal data breach

    - a description of the measures taken to deal with the breach and, where appropriate, the measures taken to mitigate any possible adverse effects.

- Regardless of reporting to the ICO, all personal data breaches will be recorded in line with Article 33(5) of the GDPR. This requires us to document the facts relating to the breach, its effects and the remedial action taken.

- We will investigate the cause of the data breach and determine how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

14. Children

Children under the age of 16 only attend the clinic with the signed consent of and accompanied by a parent or legal guardian.

Children's personal data is managed by the clinic for the legitimate purposes of making clinical decisions and providing therapeutic care, advice and onward referrals.

We do not contact children under the age of 16 to arrange or discuss appointments; all communication is through a parent or legal guardian.

15. Review

Data protection procedures will be regularly reviewed and audited in order to ensure continued compliance with the GDPR.

This policy will be reviewed at intervals of **2 years** to ensure it remains up to date and compliant with the law.

Miss Kate Stalker
Clinic Director
The Derbyshire Sporting Joint
David Lloyd Leisure, Riverside Road
Derby, DE24 8HY

Tel: 01332 369713

THE DERBYSHIRE SPORTING JOINT
Professional Proactive Physiotherapy