

## **Data Protection and Privacy Policy**

This document describes how Shona Dewar Physiotherapy Ltd, trading as Bruntsfield Physiotherapy and Sports Medicine Clinic collects and uses personal information about you during and after your working relationship with us, in accordance with UK and Scottish law and the European Union's General Data Protection Regulation (GDPR).

It applies to all our patients.

### **Contents**

1. Who are we? .....	1
2. What is Privacy? .....	1
3. What information do we collect about you? .....	1
4. Security of Information.....	2
5. What are the legal bases on which we rely? .....	2
6. How will we use the information about you? .....	3
7. Retention and Disposal of data.....	4
8. Access to your information and correction.....	4
9. Marketing .....	4
10. Reporting Breaches.....	4
11. Data Protection Officer .....	5
12. How to contact us .....	5
13. Changes to our privacy policy .....	5
14. Complaints .....	5



## **Who are we?**

Bruntsfield Physiotherapy and Sports Medicine Clinic is the trading name for Shona Dewar Physiotherapy Ltd (The Company). The Company is committed to protecting the privacy and security of your personal information.

The company is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained within this document.

This notice applies to current and former patients. This notice does not form part of any contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

## **What is Privacy?**

Privacy is the confidentiality of your personal information and it is of vital importance to us at The Company. We are registered with the Information Commissioner as required under the data protection laws in the United Kingdom and Scotland and are committed to compliance with Data Protection legislation including the European Union's General Data Protection Regulation (GDPR), legislation and regulation pertaining to medical confidentiality and the CSP/HCPC Governance guidelines.

## **What information do we collect about you?**

We collect information about you when you register with us and during your appointment.

- **Personal Data:**  
Identifiable information about you, like your name, email, address, telephone number, date of birth, gender, payment information, feedback etc. If you can't be identified (for example, when personal data has been aggregated and anonymised) then this notice doesn't apply.
- **Data Concerning Health:**  
Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about your health status. The confidentiality of your personal medical information is of paramount concern to us, The Company, and we comply with UK data protection law and all the relevant medical confidentiality guidelines.

Your confidential medical information will only be disclosed to those involved with your treatment or care, or in accordance with UK law and guidelines from professional bodies, or for the purposes of clinical audit (unless you object).

**NB: Data concerning health is not fully covered in this policy.**

## **Security of Information**

We are committed to keeping your personal information secure. We have put in place physical, electronic and operational procedures intended to safeguard and secure the information we collect. Our staff have a legal duty to respect the confidentiality of your information, and access to your confidential and medical information is restricted only to those who have a reasonable need to access it.

We take reasonable precautions and follow industry best practices to make sure it is not inappropriately lost, misused, accessed, disclosed, altered or destroyed.

On the occasion that we send personal information via email, those emails are encrypted. We will only send such information to patients themselves, medical insurance providers supporting patient treatment and other medical practitioners as necessary on a case by case basis. If you send us information via your own personal email system, all transmission of personal information and other data is done at your own risk.

Information submitted to The Company through a website is normally unprotected until it reaches us. In addition, users are also requested not to send confidential details or credit card numbers, for example, by email.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted TO our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

## **What are the legal bases on which we rely?**

The GDPR law on data protection sets out a number of different reasons a company may collect and process your personal data, including:

- **Consent**

We can collect and process your data with your consent, e.g. when you fill in our registration forms or contact us by telephone or email. When collecting your personal data, we'll always make clear to you which data is necessary in connection with a particular service. We may ask you for you for relevant information which will assist in providing you with the best possible treatment and advice.

By providing your data and/or information, or by using our website or other online or digital platforms, you consent to the use of your data and information as described or referred to in this privacy notice and the cookie policy. The provisions of The Company's social media terms and conditions may also apply.

If we make a change to any of the ways in which we process personal information, we will update this web page with an updated date displayed at the top of this page, so please check back regularly for updates.

- **Contractual obligations**

In some instances, we need your personal data to comply with our contractual obligations. For example, if you undertake a program of treatment with us which is to be paid through your insurer, we need your address details and insurance policy details in order to process payment.

- **Legal compliance**

We may be legally bound to collect and process your data. For example, if someone is involved in any criminal activity or fraud affecting The Company, we need to pass details to law enforcement.

- **Legitimate interest**

We require your data to pursue our legitimate interests in a way which might reasonably be expected as part of running our business and which does not materially impact your rights, freedom or interests.

### **How will we use the information about you?**

We use your personal information to conduct our business and to provide you with our services and to improve and extend our services. This may include:

- creating appointments and responding to your queries
- supporting your medical treatment and care
- internal record keeping and administration
- responding to requests for information where we have a legal or regulatory obligation to do so
- checking the accuracy of information about you, and the quality of your treatment or care, including auditing medical and billing information for insurance claims.
- supporting your doctor or other healthcare professional
- assessing the type and quality of care you have received and any concerns or complaints you raise, so that these can be properly investigated
- using your contact information to send you service-related information (only if you have agreed to this)
- using your contact information to give you an opportunity to complete a customer satisfaction survey
- using your contact information to conduct and analyse market research

We collect information about you to enable us to manage your appointments, accounts, for communicating with other health professionals and very occasionally to inform you of new services and products.

We will only share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

In order to maintain our digital diaries, the company uses external companies known as data processors. Our data processors are also bound by the data protection act and will only process your details in accordance with our documented instructions. We also use a third party processor to securely destroy data concerning health after a period of 8 years.

### **Retention and Disposal of data**

As a provider of medical services we The Company are legally required to maintain copies of patient medical records for a period of 8 years from the date of your last treatment. This includes your personal information. After 8 years they are securely destroyed using a third party processor.

At present electronic copies of personal information are maintained indefinitely by our data processor. As these are attached to your patient/health records you may request your details be removed after a period of 8 years. To request this information please email us at [reception@bruntsfieldphysiotherapy.co.uk](mailto:reception@bruntsfieldphysiotherapy.co.uk) or write to us at Bruntsfield Physiotherapy and Sports Medicine Clinic, 17-19 Barclay Place, Edinburgh, EH10 4HW.

### **Access to your information and correction**

You have the right to request a copy of the information that we hold about you. If you would like a copy of some or all of your personal information please email us at [reception@bruntsfieldphysiotherapy.co.uk](mailto:reception@bruntsfieldphysiotherapy.co.uk) or write to us at Shona Dewar, Data Protection Officer, Bruntsfield Physiotherapy and Sports Medicine Clinic, 17-19 Barclay Place, Edinburgh, EH10 4HW.

### **Marketing**

Occasionally, if you agree, we may use your information to contact you regarding new products or services. You have the right at any time to stop us from contacting you for marketing purposes. If you wish us to stop contacting you for marketing purposes please email or write to us.

### **Reporting Breaches**

In the case of a personal data breach, the company shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office (ICO) in accordance with the data protection act, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

This notification shall include:

- A description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach;
- A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The company shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this policy.

### **Data Protection Officer**

The Company has appointed Shona Dewar as the Data Protection Officer (DPO). If you have any queries about this policy or concerns about your data please contact us.

### **How to contact us**

Please contact us if you have any questions about our privacy policy or information we hold about you:

Data Protection Officer: Shona Dewar

By email: [reception@bruntsfieldphysiotherapy.co.uk](mailto:reception@bruntsfieldphysiotherapy.co.uk)

Or write to us at:

Shona Dewar,  
Data Protection Officer,  
Bruntsfield Physiotherapy and Sports Medicine Clinic,  
17-19 Barclay Place,  
Edinburgh,  
EH10 4HW

### **Changes to our privacy policy**

We keep our privacy policy under regular review and we will place any updates on this webpage. This privacy policy was last updated on 22 February 2024.

### **Complaints**

If you think there is a problem with the way we process your data please contact us to express your concerns as per our complaints policy ([Complaints-Procedure-Updated-24\\_10\\_2020.pdf \(bruntsfieldphysiotherapy.co.uk\)](#)).

If you remain unhappy with the way we process your data you may complain to the Information Commissioner's office (ICO). You can find out more about the ICO here: <https://ico.org.uk>

## **Review and Approval**

This policy will be reviewed annually or sooner if there are changes in legislation or best practice guidelines.

**Policy Review Date:** February 2025

**Approved by:** Shona Dewar, Clinical Director

**Date of Approval:** 22nd February 2024

By adhering to this policy, our clinic ensures to protect our patients data, compliance with legal requirements, and the provision of high-quality care to our patients.