General Data Protection Policy

First introduced September 2012 as Data Protection Policy
Review Date 8th May 2018
Next Review Due 8th May 2020

Table of Contents

.

1. STATEMENT OF POLICY

This is a statement of the General Data Protection Regulations Policy adopted by Physiotherapy2Fit Ltd. The Physiotherapy2fit General Data Protection Regulations Policy is subject to regular review to reflect, for example, changes to legislation or to the structure or policies of Physiotherapy2fit Ltd. All staff are expected to apply the policy and to seek advice when required.

Physiotherapy2fit needs to collect and use certain types of information about people with whom it deals in order to operate. This includes current and past individuals that have been referred to Physiotherapy2fit, our own employees, suppliers and others with whom we conduct business. In addition, Physiotherapy2fit may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, electronically, or other means - and there are safeguards to ensure this in the Data Protection Act 1998 and GDPR.

Physiotherapy2fit Ltd regard the lawful and correct treatment of personal information as important to the achievement of our objectives and to the success of our operations, and to maintain confidence between those with whom we deal and ourselves. We therefore need to ensure that our organisation treats personal information lawfully and correctly.

Physiotherapy2fit fully endorse and adhere to the Principles of data protection, as set out in the Data Protection Act 1998 and GDPR. In issuing this GDPR Policy, Physiotherapy2fit Ltd is also looking to comply with the spirit of the British Standard for Data Protection: BS 10012.

GDPR Policy

Personal data shall be obtained, maintained, stored, used and passed on only in strict accordance with the Data Protection Act 1998. Physiotherapy2fit Ltd is concerned about protecting personal information it gathers about employees and customers.

- Physiotherapy2fit Ltd will limit the collection of data to that which is needed for valid business purposes or to comply with the law, and any such data will be obtained only by lawful and fair means.
- Physiotherapy2fit Ltd will strive to maintain the accuracy of the personal data held.
- Physiotherapy2fit Ltd will not release personal data to a third party unless the individual/customer requests this or that law requires the disclosure.
- Physiotherapy2fit Ltd will take appropriate steps to ensure that personal data is protected from unauthorised access and disclosure, including limiting access to such data only to those employees with a business need to know.

Definitions

Personal data is defined as follows:
Data which relate to a living individual who can be identified:

- From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
- A data controller is a person who determines the purposes for which the manner in which any personal data are, or are to be, processed.
- The GDPR act covers both electronic and paper based information.
- Sensitive Data means data relating to: racial or ethnic origin; religious or similar beliefs; trade union membership; physical or mental health or sexual life; political opinions or criminal offences. This data may only be held in strictly defined situations or where explicit consent has been obtained.

.

2. THE PRINCIPLES OF GDPR

The Data Protection Act 1998/GDPR stipulates that anyone processing personal data must comply with Eight Principles of good practice. It is essential therefore that Physiotherapy2fit Ltd fully complies with it, not just to avoid prosecution and bad publicity, but to demonstrate to customers that Physiotherapy2fit Ltd operates with due diligence and responsibility. Also, all employees should bear in mind that a breach of the act can lead to claims for compensation.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

These Principles are legally enforceable.

The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and sensitive personal data.

a) Definitions

Personal data is defined as, data relating to a living individual who can be identified from:

•That data and other information which is in the possession of, or is likely to come into the
possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

- A data controller is a person who determines the purposes for which the manner in which any personal data are, or are to be, processed.
- The data protection act covers both electronic and paper based information.
- Sensitive Data means data relating to: racial or ethnic origin; religious or similar beliefs; trade union membership; physical or mental health or sexual life; political opinions or criminal offences. This data may only be held in strictly defined situations or where explicit consent has been obtained.

b) Collecting Personal Data

When collecting personal data make sure that people know;

- Who we are
- What the data will be used for
- To whom it will be disclosed

This information can be provided on an application form or something similar. It is equally important NOT to collect more personal data than is necessary.

.

c) Handling Personal Data

When handling, collecting, processing or storing personal data, ensure that:

- All personal data is both accurate and up to date

- Errors are corrected effectively and promptly
- The data is deleted/destroyed when it is no longer needed
- The personal data is kept secure at all times (protected from unauthorised disclosure or access)
- The Data Protection Act is considered when setting up new systems or when considering use of the data for a new purpose.
- Written contracts are used when external bodies process/handle the data, explicitly specifying the above requirements with respect to the data.

It is equally important NOT to:
- Access personal data that you do not need for your work
- Use the data for any purpose it was not explicitly obtained for
- Keep data that would embarrass or damage IPRS if disclosed
- Transfer personal data outside or the European Economic Area unless you have consent from the individual concerned
- Store/process/handle sensitive personal data unless you are certain you are entitled to, or consent from the individual concerned has been obtained.

d) Sensitive Data

Sensitive personal data is defined as personal data consisting of information as to:
- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition (including Medical Records);
- Sexual life;
- Criminal proceedings or convictions.

When handling personal/sensitive information, Physiotherapy2fit Ltd will, through appropriate management and the use of strict criteria and controls:-

- Observe fully conditions regarding the fair collection and use of personal information; Meet its legal obligations to specify the purpose for which information is used;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Apply strict checks to determine the length of time information is held;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred abroad without suitable safeguards;
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed
- The right of access (within 30 days)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject t automated decision-making including profiling.

In addition,
Physiotherapy2fit Ltd will ensure that:

- There is someone with specific responsibility for data protection in the

organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with; Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.
- All Physiotherapy2fit Ltd employees are to be made fully aware of this policy and of their duties and responsibilities under the Act.

.

3. PROTECTING DATA

All managers and staff within Physiotherapy2fit Ltd will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal / sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of Physiotherapy2fit Ltd must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of Physiotherapy2fit Ltd, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act
- Allow data protection audits by Physiotherapy2fit Ltd of data held on its behalf (if requested)
- Any breach of any provision of the Act will be deemed as being a breach of any contract between Physiotherapy2fit Ltd and that individual, company, partner or firm
- Indemnify Physiotherapy2fit Ltd against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation All contractors who are users of personal information supplied by Physiotherapy2fit Ltd are required to abide by the requirements of the Act with regard to information supplied by the Physiotherapy2fit Ltd.
- GDPR restricts the transfer of personal data to countries outside the EU.

Subject Access and Subject Rights

Individuals, who the data relates to, have various rights:

- To receive, on request, details of the processing relating to them. This includes any information about themselves including information regarding the source of the data and about the logic of certain 'Fully automated decisions'
- To have any inaccurate data removed or corrected
- In certain circumstances to stop processing likely to cause 'Substantial damage or substantial distress'
- To prevent the data being used for marketing or advertising

When a subject access request is received, it is important to:

- Treat the requester with courtesy and try to find out what is being sought;
- Act promptly and effectively within 30 days.
  In most cases you will not be able to charge for complying with a request unless they are manifestly unfounded or excessive.

.

4. ROLES AND RESPONSIBILITIES

GDPR means that the Physiotherapy2fit Ltd must:

- Manage and process personal data properly Protect the individual's rights to privacy Provide an individual with access to all personal information held on them
- Physiotherapy2fit Ltd has a legal responsibility to comply with the Act.
- Every member of staff that holds information about identifiable living individuals has to comply with GDPR in managing that information. Individuals can be liable for breaches of the Act.

a) All Employees

All employees are responsible for ensuring that this Policy is followed.
Employees have a responsibility to comply with the GDPR Principles and should :

- Make themselves familiar with the rules and 'best practice' of Physiotherapy2fit Ltd GDPR Policy
- Be aware and mindful of the manner in which they process information, in particular personal information left on computer screens, sending and receiving of faxes, sending and receiving of e- mails, manual records left unattended
- Ensure that information is not passed on in any unauthorised way.
- Not disclose data outside of their line of duty. If an individual is found to have permitted unauthorised disclosure they, as well as Physiotherapy2fit Ltd, could face prosecution.
- Seek guidance from their Manager if unsure about what information they are permitted to disclose
- Treat data with care and not to pass on information to unauthorised persons.
- During the course of an employee's employment with Physiotherapy2fit Ltd or on leaving, staff are reminded not to use or disclose to any other person or institution, information made available to them during the course of their employment except in the pursuance of the authorised business of Physiotherapy2fit Ltd. Such information includes details relating to patients, members of staff or the business / commercial interests of Physiotherapy2fit Ltd.
- It is the responsibility of each employee to keep Physiotherapy2fit Ltd informed of any changes in personal circumstances, including changes of address, next of kin, criminal convictions, any arrests, charges or cautions from the police authorities or change in work permit or professional registration status.
- Any breach of this Policy and Procedure may result in disciplinary action being taken. Penalties for these infractions will range from informal warnings through to dismissal:

a) Minor Misconduct – Inadvertent disclosure of privileged or confidential information.
b) Serious Misconduct – Careless disclosure of privileged or confidential information.
c) Gross Misconduct – Deliberate disclosure of privileged or confidential information to unauthorised people.

In particular, your attention is drawn to the following:

Physiotherapy2fit Ltd Employees will not release personal data to a third party unless the individual/customer requests this or that the disclosure is required by law. Physiotherapy2fit Ltd will take appropriate steps to ensure that personal data is protected from unauthorised access and disclosure, including limited access to such

data only to those employees with a business

Managers/Director

All managers / area leads are responsible for ensuring that:

- The processing of personal data in their department conforms to the requirements of the GDPR Act and this Policy.
- In particular, they should ensure that new and existing staff who are likely to process personal data are aware of their responsibilities under the Act. This includes drawing the attention of staff to the requirements of this policy, and ensuring that staff who have responsibility for handling personal data are provided with adequate training.
- Managers must also see that correct information and records management procedures are followed in their departments.

5.RELATIONSHIP WITH OTHER LEGISLATION AND PHYSIOTHERAPY2FIT POLICIES

The following Legislation (incl. Codes of Practice) and Physiotherapy2Fit Policies are linked to this Policy.

a) Legislation

The legislation listed below also refers to issues of security and/or confidentiality of personal identifiable information / data:

- General Data Protection Regulations
- Data Protection Act 1998
- Access to Health Records 1990
- Access to Medical Reports Act 1988
- Crime and Disorder Act 1998

Other Codes of Conduct that apply are: • The 2007 Rehabilitation Code

b) Other Physiotherapy2Fit Policies

6. NOTIFICATION TO THE INFORMATION COMMISSIONER

The Information Commissioner maintains a public register of data controllers.
Physiotherapy2fit Ltd is registered as such.

The GDPR requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence. To this end, the designated officers will be responsible for notifying and updating the Information Officer of the processing of personal data, within their directorate. The DP Information Officer will review the Data Protection Register with designated officers annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

To this end, any changes made between reviews will be brought to the attention of the DP Information Officer immediately.
The Data Protection Officer for Physiotherapy2Fit is Sarah Booker

7. RETENTION OF DATA

Personal data, records and notes relating to the physiotherapy/rehabilitation of adult subjects must be retained for a minimum period of 8 years to coincide with legal requirements and professional standards. For patients under the age of 18 years, records must be kept until they reach the age of 25 years.

Physiotherapy2fit Ltd will keep some forms of information for longer than others, in accordance with legal, financial, archival, or other requirements.

a) Research Purpose Exemption

Data collected fairly and lawfully for the purpose of research can be used, providing that the final results of the research do not identify the individual. Such data must not be processed to support measures of decisions with direct consequences for the individual concerned, or in a way which is likely to cause substantial damage or distress to any data subject. This exemption is only applicable to academic research, and cannot be used to provide information about an individual.

8. BREACHES TO DATA PROTECTION

Any breach of data protection will be investigated in line with the Department of Healths **Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents Gateway Ref: 13177.**

The number and categories of breaches will be brought to the attention of the Director/Caldicott Guardian. A summary of data losses and breaches will also be included in reports to the CCG.

Some breaches will be deemed following investigation to warrant disciplinary procedures. This will be the responsibility of the Director.
The ICO need to be contacted when there is a breach which is likely to result in a risk to the rights and freedoms of individuals – if for example it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. This needs to be done within 72 hours of discovering it "where feasible".

9. CONTACTS

Under the GDPR Act, any individual may write to the Director of Physiotherapy2fit Ltd at the address listed below and request a copy of the information which we hold about them. If the details are inaccurate you can ask us to amend them.

Physiotherapy2fit Ltd has 30 days from the receipt of the request in which to comply.

Requests must be made in writing. Physiotherapy2fit Ltd will be careful not to disclose information to inappropriate parties and also needs to be particularly aware of any other confidentiality obligations to third parties. Legal advice might be necessary if the situation is complex.

Director and Lead Clinician, Physiotherapy2fit Ltd, 19 Bradley Drive, Sittingbourne, Kent, ME10 1RB.