Milestones

Multidisciplinary
Neurorehabilitation Clinic

Milestones Clinic Ltd

Data Protection Policy

Review Schedule: *Every 2 years*
Next review date: *June 2020*
Owner: *Sally de la Fontaine – Director*

This document outlines our legal requirements under the General Data Protection Regulations (GDPR) and the processes for how Milestones Clinic Ltd meets them

Implementation and Quality Assurance

1. *Implementation is immediate and this policy will stay in force until any alterations are formally agreed. It will be reviewed every two years by the Directors, sooner if legislation, best practice and / or if other circumstances indicate this is necessary*

2. *All of Milestones Clinic Ltd staff and their associates are required to follow this policy at all times*

3. *The Directors (Controllers) have overall responsibility for data protection within Milestones Clinic Ltd but each individual (Processor) processing data is acting on the Controllers behalf and therefore has a legal obligation to adhere to the regulations*

4. *When providing physiotherapy to clients under the management of a case manager then Milestones Clinic Ltd and the Case Management company act as joint controllers*

Summary:

The GDPR and Data Protection Act 2018 replace the Data Protection Act 1998 with an updated and strengthened data protection framework.

The GDPR applies to 'personal data'. This means data which relate to a living individual who can be identified from these data, or from these data and other information which is in the possession of, or is likely to come into the possession of the 'data controller'.

Personal data include, for example, name, address, email address, telephone numbers, NHS number or a computer IP address.
Personal data which reveal the health status of an individual are 'special category' data under GDPR.

The term confidential health data is used throughout the guidance and is intended to encompass 'special category' health data under the GDPR and data which are subject to the common law duty of confidentiality.

Milestones, 39A South Avenue,
Egham, Surrey TW20 8HQ

01784 457 520

sally@milestonesclinic.co.uk
www.milestonesclinic.co.uk

hcpc registered
www.hcpc-uk.org

Milestones

Multidisciplinary
Neurorehabilitation Clinic

From 25 May 2018, the Data Protection (Charges and Information) Regulations 2018 requires every organisation or sole trader who processes personal information to pay a data protection fee to the ICO, unless they are exempt.

Provision of direct care when explicit consent is not required:

1. *Lawful basis for processing 'special category' data is deemed necessary for the compliance with a legal obligation to which a controller is subject*

2. *Special category condition for processing for direct care is that processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems and services*

Purposes other than direct care:

Where we receive a request for confidential health data from an insurance company, solicitor or employer (or similar third party) the lawful basis and lawful condition for processing will be explicit consent i.e. freely given, specific, informed and unambiguous indication of the data subject's agreement

Data controller responsibilities:

1. *Process personal data fairly, lawfully and in a transparent manner*

2. *Obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner which is incompatible with the purpose or purposes for which is was obtained*

3. *Ensure that the personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held*

4. *Ensure that the personal data is accurate and, where necessary, kept up to date*

5. *Ensure that the data is not kept for any longer than necessary for the purpose it was obtained, this may include indefinitely should that be appropriate*

6. *Ensure that the personal data is kept secure*

hcpc registered
www.hcpc-uk.org

7. *Ensure that the personal data shall not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights and freedoms of the individuals to whom the personal data relates*

Consent:

Milestones Clinic Ltd, must record service users' explicit consent to storing confidential health data on file and for the purposes of the regulations, this relates to:

a. *The racial or ethnic origin of the client*
b. *Their political opinions*
c. *Their religious beliefs or other beliefs of a similar nature*
d. *Whether they are a member of a trade union*
e. *Their physical or mental health or condition*
f. *Their sexual life*
g. *The commission or alleged commission by them of any offence, or*
h. *Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings*

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

As a general rule Milestones Clinic Ltd will always seek consent where confidential health care data is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

If confidential health data needs to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Director for advice.

Special categories of personal information collected by Milestones Clinic Ltd will, in the main, relate to service users' physical and mental health.

<u>Obtaining Consent:</u>

Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records: face-to-face; written; telephone; email

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing of were to be undertaken.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. If the subject is less than 18 years of age then parental / guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by Milestones Clinic Ltd then this should be discussed with the Director at the earliest opportunity.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information:

1. *It is an offence to disclose personal information 'knowingly and recklessly' to third parties.*
2. *It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.*
3. *Service users may also consent for us to share confidential health data with other helping agencies on a need to know basis.*
4. *A client's individual consent to share information should always be checked before disclosing personal information to another agency.*
5. *Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the Director should first be sought.*
6. *Personal information should only be communicated within Milestones Clinic Ltd staff and associates on a strict need to know basis. Care should be taken that conversations containing confidential health data may not be overheard by people who should not have access to such information.*

Registered Office: 9 St.George's Yard, Castle Street, Farnham, Surrey, GU9 7LW, UK | Registered in England and Wales 6420187

Use of Files, Books and Paper Records:

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data.

Paper records should be kept in locked cabinets / drawers overnight and care should be taken that confidential health data is not left unattended and in clear view during the working the day. When transporting documents they should be carried out of sight in a bag which is shut and kept on your person.

If your work involves you having confidential health data at home or in your car, the same care needs to be taken. Documents should not be kept in open view (e.g. on a desktop) but kept in a file in a drawer or filing cabinet, the optimum being a locked cabinet but safely out of sight is a minimum requirement.

Disposal of Scrap Paper, Printing or Photocopying Overruns:

Be aware that names /addresses / phone numbers and other information written on scrap paper are also considered to be confidential.

Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

If you are transferring papers from your home, or your client's home, to the office for shredding this should be done as soon as possible.

Computers:

Computer access to confidential health data is restricted by password to authorised personnel only.

Firewalls and virus protection to be employed at all times to reduce the risk of hackers accessing systems and thereby obtaining access to confidential records.

Where mobile devices are used the device must be password protected

WordPress:

We use a third party service, WordPress.com, to publish our website. We use a standard WordPress service to collect anonymous information about users' activity on the site, for example the number of users viewing pages on the site, to monitor and report on the effectiveness of the site and help

us improve it. WordPress requires visitors that want to post a comment to enter a name and email address.

Direct Marketing:

Direct Marketing is a communication that seeks to engage new clients and promote Milestones Clinic Ltd services. The communication may be in any of a variety of formats including mail, telemarketing and email. Milestones Clinic Ltd will not share or sell its database(s) to outside organisations.

The following statement is to be included on any forms used to obtain personal data: We promise never to share your information to other organisations or businesses unless you have consented to this. You can opt out of our communications at any time by telephoning 01784 457 520, writing to The Director, Milestones Clinic Ltd, 39A South Avenue, Egham, Surrey TW20 8HQ or emailing andy@milestonesclinic.co.uk

Privacy Statements

Any documentation which gathers confidential health data should contain the following Privacy Statement information:

- *Explain who we are*
- *What we will do with their data*
- *Who we will share it with*
- *Consent for marketing notice*
- *How long we will keep it for*
- *That their data will be treated securely*
- *How to opt out*
- *Where they can find a copy of the full notice*

Personnel Records

The Regulations apply equally to associates and staff records.

Confidentiality

When sending emails to outside organisations, e.g. social worker or hospital staff, care should be taken to ensure that any identifying data is removed and that codes (e.g. initials or identifying code number etc.) are to be used.

Confidential health data should be written in a separate document which should be password protected before sending.

Any paperwork kept away from the office (e.g. clients notes or reports) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (e.g. on a desktop) but

kept in a file in a drawer or filing cabinet, the optimum being a locked cabinet but safely out of sight is a minimum requirement.

If you are carrying documents relating to a number of clients when on a series of home visits, you should keep the documents for other clients out of sight in a bag which can be securely closed or zipped up.

Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a client's home with the correct number of documents and that you haven't inadvertently left something behind.

What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to the Director who will review our systems, as a Quality Assurance & Systems Manager, to prevent a reoccurrence.

Information Commissioner

There is a time limit for reporting breaches to ICO so the QA & Systems Managers should be informed without delay.

Any deliberate or reckless breach of this Data Protection Policy by a member of staff or associate may result in disciplinary action which may result in dismissal / cessation of contract.

The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing their data:

1. *Confidential health data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).*

2. *Data cannot be used for the purposes of direct marketing of any goods or services if the client has declined their consent to do so.*

3. *Individuals have a right to have their data erased and to prevent processing in specific circumstances:*

- *Where data is no longer necessary in relation to the purpose for which it was originally collected*
- *When an individual withdraws consent*
- *When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing*
- *Personal data was unlawfully processed*

4. *An individual has a right to restrict processing*

5. *Clients can ask, in writing to the data controller, to see all personal data held on them, including e-mails and computer or paper files. The data controller must comply with such requests within 30 days of receipt of the written request.*

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence:

- *The unlawful obtaining of personal data*
- *The unlawful selling of personal data*
- *The unlawful disclosure of confidential health data to unauthorised persons*

Further information is available at https://ico.org.uk

The Information Commissioner's office is at:
Information Access Team
Information Commissioner's Office
Wycliffe House Water Lane
Wilmslow
Cheshire SK9 5AF