PONHC
Prestwood Osteopathic & Natural Health Centre

Data Protection Policy

Key Details

- Policy prepared and approved by Philip Allen (Principal) for Prestwood Osteopathic & Natural Health Centre Ltd (PONHC) and Caren Thompson (Practice Manager)
- Policy became operational on 01/05/2018
- Policy will be reviewed on 01/05/2019

Introduction

PONHC obtains information from patients for the purpose commensurate with the patient's intention in contacting us. Personal details are taken for identification and contact. Further personal details are obtained for the purposes of medical help. Contact information may be used to inform patients of services that we believe would be of interest to them but will not, in any circumstance, be passed to a third party. Medical histories will be shared with legal representatives and other medical practitioners only under signed authority from the patient.

Why this policy exists

This data protection policy ensures that PONHC

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and patients
- Is open about how it stores and processed individuals' data
- Protects itself from the risk of a data breach

Data Protection Law

The Data Protection Act 1998 and the EU General Data Protection Regulation 2018 describes how organisations, including PONHC, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and up to date
5. Not be held for any longer than is necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area unless that country or territory also ensures adequate levels of protection

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- The head office
- Any satellite offices of PONHC
- All staff and volunteers of PONHC
- All contractors, suppliers and other people working on behalf of PONHC

It applies to all the data the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 & EU GDPR 2018. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

Data Protection Risks

This policy helps to protect PONHC from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

- Reputational damage. For instance, the company could suffer if hackers gained access to sensitive data.

Responsibilities

Everyone who works for or with PONHC has some responsibility for ensuring data is collected, stored and handled appropriately.

Each individual that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- Director and Principal, Philip Allen, is ultimately responsible for ensuring that PONHC meets its legal obligations.
- The Data Protection Officer, Caren Thompson, is responsible for:
    - Keeping Philip Allen updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection and related policies in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions form staff, practitioners and anyone else covered by this policy.
    - Dealing with request from individuals to see the data PONHC holds about them (also called 'Subject Access Requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure hardware and software is performing properly.
    - Evaluating any third-party services the company is considering using to store or process data, for instance, diary services or cloud computing services.
    - Approving data protection statements attached to communications such as email and letters.
    - Addressing data protection queries from journalists or media outlets like newspapers.
    - Where necessary working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work. Data should not be shared informally. When access to confidential information is required, employees and practitioners must request it from the Practice Manager.
- PONHC will supply training to all employees and practitioners to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees and practitioners should request help from their line manager/principal if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Practice Manager or Principal.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drivers and servers and should only be uploaded to an approved cloud computing service.
- Servers containing personal information should be sited in a secure location, away from general office space.

- Data should be backed up frequently. Those back-ups should be tested regularly, in line with the company's standard back up procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones.
- All servers and computer containing data should be protected by approved security software and a firewall.

Data Use

Personal data is of no value to PONHC unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- If Data needs to be sent by email we will send a request for permission to send and post the data by reply.
- Personal data should never be transferred out of the European Economic Area.
- Employees/Practitioners should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Accuracy

The law requires PONHC to take reasonable steps to ensure that data is kept accurate and up to date.

The more important it is, that personal data is accurate, the greater the effort PONHC should put into ensuring its accuracy.

It is the responsibility of all employees and practitioners who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff/practitioners should not create any unnecessary data sets.
- Staff/practitioners should take every opportunity to ensure that data is updated. For instance, by confirming a customer's details when they call.

- PONHC will make it easy for data subjects to update the information PONHC holds about them. For instance, via the online diary.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Principal/Practice Manager's responsibility to ensure marketing databases are checked against industry suppression files (such as advertising standards in relation to complimentary health) every six months.

Subject Access Requests

All individuals who are the subject of personal data held by PONHC are entitled to:

- Ask what information the company holds about them and why?
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting their information, this is called a Subject Access Request.

Subject Access Requests from individuals should be made by email, or in writing and be addressed to the Practice Manager of PONHC. The Practice Manager can supply a standard request form, though individuals do not have to use this.

Individuals will be charged £10 per Subject Access Request. The Practice Manager will aim to provide the relevant data within 40 days.

The Practice Manager will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for Other Reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances PONHC will disclose requested data. However the Practice Manager will ensure that a request is legitimate, seeking assistance from the Principal and legal advisors where necessary.

Providing information

PONHC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

This document is to be displayed on our notice board in the Practice, and a copy is available upon request.

An electronic version of this is also available on the PONHC website, and on our Facebook page.