Pennine Medical Centre

DATA PROTECTION POLICY

Written By: Joanne Cassinelli – Practice Manager
Authorised By: Dr Capuano – GP
Review Date: 30/8/19

Introduction

Pennine Medical Centre needs to have a Practice Privacy Policy to demonstrate compliance with DPA 2018 and GDPR. This policy is that document. It sets out the general arrangements by which Pennine Medical Centre will be compliant under the various Articles of GDPR and the UK DPA 2018.

Pennine Medical Centre is the term used in this document to describe an NHS general practice operating under contract with NHS England plus Oldham CCG.

The contract is a GMS contract.

The Data Controller on the date of the adoption of this policy was Pennine Medical Centre

As an NHS general practice providing services under contract to NHS England plus Oldham CCG, we process personal and special category data relating to our staff and those we treat, registered patients and others, internally and with other organisations external to the practice. We also hold data on other types of customers, suppliers, business contacts and other people we have relationships with or may need to contact.

We are also required by certain laws to disclose certain types of data to other organisations on a regular basis such as NHS Digital, or Public Health England or NHS England plus Oldham CCG.

We are also required by certain laws to disclose certain types of data to other organisations on an event by event basis, such as CQC or the General Medical Council

These processing activities are described in detail in our Practice Privacy Notice which can be found on the shared drive/in the waiting rooms and practice website.

Why this policy exists

Pennine Medical Centre understands that with the advent of modern technologies, and in particular “social media type communications” the emphasis of data processing needs to be refocused to a default of protection and move forward only when disclosure is of benefit to the data subject.

Pennine Medical Centre is open about how it stores and processes personal data and protects itself from the risks of a data breach

General

This policy applies no matter how the data is stored; electronically as text, documents, images or in tables, on paper or on other materials.

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

Personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways

Policy scope

This policy applies to all our staff, clinical and non-clinical, to everyone who works in Pennine Medical Centre.

It applies to all the personal data that we process.

Responsibilities

Everyone who works for or with Pennine Medical Centre has shared responsibility for ensuring data is collected, stored and handled appropriately. Each person that handles personal data in this organisation must ensure that it is handled and processed in line with this policy and data protection principles. Some people have key responsibilities

The contract holders are ultimately responsible for ensuring that Pennine Medical Centre meets its legal obligations.

The Data Protection Officer, Jane Hill, is responsible for:

- Keeping the contract holders, partners, doctors and all staff informed about data protection responsibilities, risks and issues, where necessary pre-emptively. Providing advice to the data controllers when requested.
- Advising on the need for and generation of DPIAs.
- Reviewing all data processing procedures, practices and policies as well as this policy on an annual basis.
- Arranging appropriate and relevant in-house training for the people covered by this policy.
- Keeping up to date to an appropriate standard in all matters relevant to the role.
- Remaining independent and impartial and ensuring that any conflicts are reported to the partners.
- Handling data protection questions from staff and anyone else covered by this policy.
- Acting as the point of contact for data subjects.
- Dealing with requests from data subjects relating to their rights under CLDoC and GDPR including ensuring there is a compliant SAR and TSAR process.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Acting as the interface to the ICO.
- Ensuring that the practice completes the IG Toolkit each year.

The IT manager, Joanne Cassinelli, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and reviews to ensure security hardware and software is functioning properly.
- Liaising with the CCG provided IT infrastructure support services.
- Ensuring that cyber security recommendations are implemented and deployed.
- Advising the DPO on any technical matters relating to GDPR.

The Practice manager, Joanne Cassinelli, is responsible for the implementation of this policy.

The Data Controller(s) will ensure that the DPO has an environment in which the DPO can operate independently and without limitation. They will also involve the DPO in all relevant issues, provide support and resources for the DPO to carry out the tasks noted in this policy, including training and knowledge updating. They will not issue the DPO with any instructions or place any constraints relating to their DPO role. They will allow data subjects to access the DPO. Not allow the DPO to be conflicted by other tasks, jobs or responsibilities that they may have.

General staff guidelines

The practice will provide training to all employees to help them understand their responsibilities when handling data. Employees should keep all data secure, by taking sensible precautions and following the practices procedures and policies. NHS smartcards, Passwords and logins must be used whenever possible and they should never be shared or borrowed. Whenever a screen is left programs that handle patient data should be closed. Personal data should not be disclosed to unauthorised people, either within the company or externally. Employees should request help from the practice manager, Caldicott Guardian or the data protection officer if they are unsure about any aspect of data protection. All employees will have a privacy and data protection clause added to their contracts.