Crown Heights Medical Centre	
DATA PROTECTION POLICY	
REVIEW DATE:	**25.10.2021**
REVIEWED BY:	**C Sims DPO**
NEXT REVIEW:	**01.10.2022**

Summary

Policy prepared by: P Butterworth

Approved at: CHMC Partners Meeting

Held on: 07/12/2021

Effective from: 07/12/2021

Introduction

Crown Heights Medical Centre ("we" or "us") needs to have a Practice Privacy Policy to demonstrate compliance with the Data Protection Act (DPA) 2018 and the UK GDPR. This policy is that document. It sets out the general arrangements by which we will be compliant under the various Articles of GDPR and the UK DPA 2018.

Crown Heights Medical Centre is the term used in this document to describe an NHS general practice operating under contract North Hampshire CCG (NHCCG).

The contract is a PMS contract.

The Data Controller on the date of the adoption of this policy was Crown Heights Medical Centre.

As an NHS general practice providing services under contract to NHCCG 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 NHCCG.

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, and others, are described in detail in our Practice Privacy Notice.

Why this policy exists

We understand that with the advent of modern technologies, and in particular in the age of big data and ever more technical and complex ways to share and communicate digitally, the emphasis of data processing needs to be refocused to a default of protection and move forward only when disclosure is lawful, informed, controlled, and of benefit to the data subject.

For organisations such as CHMC, who want to build patient trust in how they collect and use personal data, the opportunities to improve their organisation and the services they offer, through the GDPR, are enormous.

We are open about how we store and process personal data and protect ourselves 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, in line with the DPA and the Common Law of Confidentiality (CLC)
- 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 Crown Heights Medical Centre.
It applies to all the personal data that we process.

Responsibilities

Everyone who works for or with us 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 we meet our legal obligations.

The Data Protection Officer :*Caroline Sims,* 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 herself up to date to an appropriate standard in all matters relevant to his 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
- Dealing with requests from data subjects relating to their rights under CLC and GDPR
- 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 DSP Toolkit each year

The IT manager: 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
- Consulting with the DPO on any technical matters relating to GDPR

The Practice manager: *Paul Butterworth*, is responsible for

- The implementation of this policy

Crown Heights Medical Centre:

- ☐ will ensure that the DPO has an environment in which the DPO can operate independently and without limitation
- ☐ will 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
- ☐ will ensure that the opinion of the DPO must always be given due weight
- ☐ will not issue the DPO with any instructions or place any constraints relating to their DPO role
- ☐ will allow data subjects to access the DPO
- ☐ will not allow the DPO to be conflicted by other tasks, jobs or responsibilities he may have, such as tasks, jobs or responsibilities outside of OHG
- ☐ will comprehensively record and thoroughly document any reasons for acting against the advice of their DPO

Designation of the DPO

- ☐ Crown Heights Medical Centre is the data controller, and as such controls the data processing. No individual GP partner is the data controller, nor is registered with the ICO as such.The practice should have access to a Data protection officer to provide expert support and guidance.

Accordingly:

- ☐ OHG has designated Caroline Sims to be the Data Protection Officer for this organisation from 1 October 2021
- ☐ This decision can be reviewed at anytime in the future should circumstances change or arise, or further official guidance be produced that necessitates it

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 or locked
- ☐ Personal data should not be disclosed to unauthorised people, either within the company or externally
- ☐ Employees should request help from the practice manager or Caldicott Guardian/DPO if they are unsure about any aspect of data protection
- ☐ All employees will have a privacy and data protection clause added to their contracts

Full details of the above can be found in our information security policy

Ongoing maintenance of the policy

1. Paul Butterworth will be responsible for ensuring that the policy is maintained accordingly.

Freedom of information

2. This policy will be available if requested under the FOI Act.

3. This policy will be downloadable from our website.