Source & Version	Date Published	Review Status	Review Due	Review Cycle	Reviewed By	**MORETONHAMPSTEAD HEALTH CENTRE**
2.7.2	Aug 2014	Mar 2023	Mar 2024	1 yrs	KB	

CONFIDENTIALITY – PATIENT DATA

Introduction

This document sets out the arrangements in the practice for the confidentiality of patient data. The Practice complies with the Data Protection Act and GDPR regulations 2018.

The Practice's Responsibilities

The practice will ensure that employees fully understand all their responsibilities regarding confidential data, by ensuring employees undertake Information Governance training and sign a written statement of the responsibilities they are undertaking towards the security of all data within the surgery. Competency will be assessed as an ongoing process and as part of the appraisal process. The practice will complete and submit the DSP Toolkit self-assessment on an annual basis.

The practice will also ensure that arrangements are in place for the confidential disposal of any paper waste generated at work. Care should be taken to ensure that the company are accredited to destroy sensitive papers. Records should be kept of the registration of the company and a log of collections.

The practice strictly applies the rules of confidentiality and will not release patient information to a third party (other than those involved in the direct care of a patient) without proper valid and informed consent, unless this is within the statutory exempted categories such as in the public interest, or if required by law, in which case the release of the information and the reasons for it will be individually and specifically documented and authorised by the responsible clinician.

The practice follows the Health and Social Care Information Centre document "A Guide to Confidentiality in Health and Social Care, Sept 2013".

Leaflet Wording (Patient Information Leaflet or Poster)

All patient information is confidential and we comply fully with the Data Protection Act and Caldicott principles. All employees in the practice have access to this information in relation to their role, have confidentiality clauses in their contracts of employment and have signed a confidentiality agreement. All staff members adhere to the Confidentiality: NHS Code of Practice 2003.

To ensure safe and effective care, patients' information may be shared with other parties within the care team who are involved in their direct care. Where a patient wishes information not to be shared within the team providing direct care, then they must discuss with their GP or the Practice Manager or Deputy Manager and decide on the most appropriate way to achieve this.

Patient information will not be shared outside of the direct care team without consent being sought. An individual has the right to refuse to have their information disclosed, although this may have an impact on their care, and their wishes will be complied with.

It is imperative that when it is right to release details to 3rd parties that the information only includes what has been asked for and not necessarily the full record.

Patients have a few options regarding the types of data opt-outs available to them. Information relating to NHS data extractions changes regularly and up-to-date information regarding the latest data opt-out options are available on the practice website on the "How Your Data is Used, Consent and Your Options" page, or by visiting NHS Digital.

Use of Online Consultation/Video-conferencing software (inc. MS Teams)

Video sharing/conferencing apps such as Skype, Whatsapp or Microsoft Teams can be used for private 1:1 chats and group chats without the need to create a team. Any instant messages (IMs) received by a user whilst offline will be available next time that user goes online.

Conversation history and chats remain, even after closing the application. Users must not share sensitive information within a chat unless it is intended for all invited participants. Invited participants will be able to read the chat even if they do not join the meeting, or if they have already been disconnected. Use a separate email or Teams chat for private conversations amongst a sub-group of colleagues.

To ensure we keep Personal Confidential Data (PCD) secure however, we need your assistance so that Teams is used correctly, both safely and securely. It is practice policy to only use NHSMail or our Clinical system to discuss and manage patient care and which may require reference to Personal Confidential Data. To maintain full awareness of the need to minimise the use of Personal Confidential Data the following general guidance applies:

Minimise the use of PCD (Personal Confidential Data).

- Only send PCD via instant message where absolutely necessary, use NHSMail to NHSMail (nhs.net) in the first instance.
- If it is essential to send PCD via Teams, then it must only be sent in an encrypted and password protected attachment from a CCG device.
- However, PCD can be safely verbally disclosed during video and voice conferences, but
- PCD should NOT be openly used if the Teams meeting is being recorded

If you choose to access on personal devices then ensure the device meets the following criteria

- Device is encrypted
- Device is fully security updated (Patched)
- Device requires authentication (i.e. 6 Digit PIN, Complex Password, Fingerprint, FaceID)

CCTV

There is no CCTV installed at the practice.

Protection against Viruses

Data is vulnerable to loss or corruption caused by viruses. Viruses may be introduced from floppy discs, CD-ROM/DVD-ROM, other storage media and by direct links via e-mail and web browsing.

Precautions to be taken

- Virus protection software is installed on ALL computer equipment.
- The supplier of our clinical software manages the anti-virus software version control and ensures it is regularly updated.
- New programmes should not be downloaded without the permission of the IT or practice manager. This reduces the risk of malware being downloaded and affecting the computer.
- When releasing any written data electronically it is best practice to see that the format is in PDF form.

Resources

Confidentiality: NHS Code of Practice
Cyber Security Policy {x}
Confidentiality Clause Staff Contracts {x
Data Protection Policy {x}
Subject Access Request Policy {x}