

Data Protection Policy

Introduction

The Practice is a 'data controller' and provides a range of services to support patient care.

Policy

The general principles underlying the use and sharing of personal information follow the Caldicott principles and data protection principles

- The purpose of using confidential information should be justified
- Only use it when absolutely necessary
- Use the minimum identifiable information for that purpose
- Access should be on a strict need to know basis only
- Everyone must understand their responsibilities to protect information
- Everyone must understand and comply with the law Personal Information

Data protection principles: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/>

Personal Information

The term 'personal information' refers to any information held about an individual who can be identified from that information.

Any information, clinical or non-clinical, held about an identifiable individual must be treated as confidential and must not be made available to anyone who is not entitled to see it.

People have a legal right to choose who has access to their personal information and how it may be used.

Staff should only have access to personal information on a justifiable need to know basis in order for them to perform their duties.

Basic Principles

Any personal information given for one purpose must not be used for another purpose without the consent of the individual concerned because that use may breach confidentiality.

Every member of staff has an obligation to protect confidentiality and a duty to verify the authorisation of another person to ensure information is only passed on to those who have a right to see it.

The rules are there to protect the individual service user and the service provider from breaches of confidentiality, but they should not be applied so rigidly that they are impractical to follow or detrimental to the care of the individual concerned.

All staff should understand their responsibility to protect the confidential information they collect and use and follow the rules and guidance available to them.

If you are unsure about whether to disclose information, consult the Data Protection Officer.

Duty of Care

All members of staff must take reasonable care to protect the physical security of confidential information from accidental loss, damage or destruction and from unauthorised or accidental disclosure.

For example:

- Data held on computers, laptops or on disk should be kept physically secure and password protected
- Do not use someone else's password to gain access to information held on computers
- Always log off when leaving a computer unattended for any length of time
- Medical records should be kept secure and never left unattended in public areas
- Confidential information should only be faxed when there is no alternative and immediate receipt is absolutely necessary for clinical purposes. 'Safe Haven' (1) procedures should be followed
- Envelopes containing patient/client confidential information must be securely sealed, marked 'Private and Confidential' and clearly addressed to a known contact
- Telephone validation procedures (2) must be followed to confirm the identity of telephone callers before information is given to them
- Patient/client information must not be transmitted by email without the use secure end to end servers

If in doubt always seek advice from the Management team.

Legislation

Data Protection Act 2018

There are 7 Data Protection principles, which regulate the use of person identifiable data (personal data). The Practice is required to demonstrate compliance with these at all times.

Article 8: Everyone has the right to respect for his private and family life, home and correspondence.

Common Law Duty of Confidence

Information obtained for one purpose should not be used for another purpose without the express or implied authorisation (consent) of the provider of that information.

Freedom of Information Act 2000

The Act gives a general right of access to all types of recorded information held by public authorities, sets out exemptions from that right and places a number of obligations on public authorities.

Data Protection Registration

The Practice is registered with the Information Commissioners Office

Data Protection Officer

The Data Protection Officer for the Practice is Ruth Quinn. She can be contacted on: nhsgm.gmgpdpo@nhs.net

The role of the Information Commissioner's Office

The Information Commissioners Office has specific responsibilities for the promotion and enforcement of the Data Protection Act.

Under the Data Protection Act, the Information Commissioner may:

- Serve information notices requiring data controllers to supply him with the information he needs to access compliance.
- Where there has been a breach, serve an enforcement notice (which requires data controllers to take specified steps or to stop taking steps in order to comply with the law).