# Staines Road Surgery

## Confidentiality Policy and Procedure

## Purpose

- To set out the obligations for all those working at the practice regarding the confidentiality of patient information held at the Practice.

- To ensure that data is kept safe from intrusion

- There is no discussion or disclosure of information to a third party without explicit agreement

- Transfer of data between co-operating service providers is sufficient for service provision, restricted to relevant material, and safe.

## Applicable to:

This policy is relevant to, and must be adhered to, by all staff including individuals on training placements, sub-contractors, peripatetic members of staff and all visitors/observers on the premises.

## Policy and Procedure

- The duty of confidentiality applies to all patients regardless of race, gender, social class, age, religion, sexual orientation, appearance, disability or medical condition as well as to patients who lack the capacity to give or withhold their consent to disclosure of confidential information

- *GMC publication `Confidentiality* (2009)` sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. All members of the team will be familiar with this document and any future editions.

- There is advice on assessing a patient's mental capacity in GMC guidance *Consent: Patients and doctors making decisions together*` and in the `*Adults with Incapacity (Scotland) Act 2000 and Mental Capacity Act 2005*` codes of practice.

- It is the responsibility of the Practice Manager to keep up-to-date with the above GMC publications and include the principles in both Contracts of Employment and Practice Induction programmes.

- Basic tenets for all staff are –

    - That the Practice provides a safe and private place for any discussions with a patient.

- That information about patients is treated as confidential and only used for the purposes for which it is given. All patient identifiable health information must be treated as confidential information, regardless of the format in which it is held. It is possible to use Information which is effectively anonymised with fewer constraints.
- Ensure that confidential information can be stored securely on the premises and that there are processes in place to guarantee confidentiality
- Prevent information from being accidentally revealed and prevent unauthorised access by keeping information secure at all times. This includes:

  (i) Refraining from discussing confidential information in a location or manner that allows it to be overheard and ensuring that telephone conversations with, or about, a patient cannot be audible in public areas.
  (ii) Handling patient information from another source sensitively and confidentially
  (iii) Never allowing confidential information to be visible in public places. Ensuring that computers are passwords protected and staff 'log out' when not using the computer.
  (iv) Ensuring that staff only access confidential information about a patient when it is necessary as part of their work
  (v) Ensuring confidential information is not removed from the premises unless it is necessary to do so in order to provide treatment to a patient and that appropriate technical safeguards are in place and there is agreement from the information governance lead or Caldicott Guardian.
  (vi) Not using any portable device to store or transfer sensitive data, unless it is encrypted and taken by secure courier to its destination.
  (vii) The use of sealed envelopes for any postal communication with patients.

  In exceptional circumstances, it may be justified to make confidential patient information known without consent if it is in the public interest or the patient's interest.

Any breach of confidence will be reported to the relevant professional bodies to be investigated.

- When a decision is taken to disclose information about a patient to a third party, due to safeguarding concerns and/or public interest, the patient should be informed and asked for their consent before the disclosure, unless it would be unsafe or impracticable to do so. In the circumstances that consent cannot be sought, there must be very explicit reasons for sharing the information and these must be justifiable.

  Disclosure of confidential information to a third party, concerning a patient, must be made to the appropriate person or organisation and in accordance with the principles of the Data Protection Act 1998, the NHS Confidentiality Code of Practice and the GMC's Good Medical Practice.

  Limited Reasons for disclosure are –
  - With the written agreement of the patient, for insurance purposes or when involved in a complaint.
  - On referral to another Provider.
  - In the wider public Interest, involving serious risk to the public or serious crime. The critical exceptions are updated by the GMC and may include

reporting concerns to the DVLA, reporting gunshot and knife wounds and serious communicable diseases. The relevant professional advice should be considered and further advice sought if unsure.

- By Court Order, but only the minimum required to comply.

Specific examples of when NOT to disclose –

- Request from a school about the attendance of a child
- Request from a parent (unless sure of being Legal Guardian) about the attendance of a child
- Request from a solicitor for information, or someone acting on behalf of a third party
  Request from a family member, even a spouse, about the attendance of a patient, or to discuss treatment

- Patients have a right of access to their records. Copies must be produced within 40 days of written request. A fee may be charged, in line with Data Protection advice.

The policy is subject to the provisions set out in the legislation and guidance listed below:
Data Protection Act 1998: The Information Commissioners' Office guide to data protection
The Department's Code of Practice for Records Management (Part 2)
Human Rights Act 1998
The Common Law Duty of Confidence
Access to Health Records Act 1990
Confidentiality: NHS Code of Practice 2003
NHS Care Record Guarantee 2009
Annex 1 Agreed ways to document, copy, store and transfer information in the ways agreed with other providers

- The policy will be reviewed regularly, and updated where necessary, to ensure that it remains effective and relevant.