Data Protection & Information Governance Policy

Purpose and Scope
To ensure that good security controls and procedures are maintained for all information created, stored and processed by the Practice, and in particular that compliance with Data Protection legislation is observed.

These procedures apply to all employees, temporary staff, volunteers, contractors and other users accessing any of the Practice information systems, wherever the user or system may be situated.

Data Protection Act Registration and Notification
The Practice has a dedicated Information Governance (IG) Lead. The IG Lead has specific roles and responsibilities in relation to the protection of personal data.

The Practice is appropriately registered with official bodies in respect of data protection, for example the Information Commissioner (ICO).

The IG Lead or their formally assigned responsible person monitors any disclosures of personal information to ensure there is a legitimate basis for the disclosure.

As per guidance from the ICO, Personal data must be:

a) Processed fairly, lawfully and transparently
b) Collected for specified, explicit & legitimate purposes
c) Adequate, relevant and necessary
d) Accurate & where necessary, up to date
e) Kept in identifiable form for no longer than necessary
f) Processed securely

The ICO suggests there are 6 legal basis for processing personal data as follows:

i) Consent of the data subject
ii) Contract with data subject
iii) Legal obligation on data controller
iv) Vital interests of any natural person

v) Task carried out in public interest / exercise of official authority
vi) Legit interests of data controller except where overridden by rights and freedoms of the data subject

Consent is required should none of the above apply. Consent should be/contain:

- Clear, affirmative action
- Freely given
- Granular
- No pre-ticked boxes
- Keep records
- Right to withdraw

Under GDPR, an individual is granted the following rights:

i) Right to be informed
ii) Right to access
iii) Right to rectification
iv) Right to erasure
v) Right to restrict processing
vi) Right to data portability
vii) Right to object
viii) Rights in respect of automated decisions and profiling

Compliance with the above is the responsibility of the IG Lead.

The Practice informs patients how their information is used, who may have access to that information, and details their own rights to see and obtain copies of their records. No personal data is transferred to any country outside of the EEA, unless adequate levels of protection are in place.

Data Quality
The Lead Partner is responsible for ensuring that:

All data held is accurate and up-to-date, the minimum necessary and relevant to the purpose.

Subject Access Requests

Under the Data Protection Act any individual has a right to 'see' personal information the organisation is holding about them. This includes patients requesting to see their medical records and staff requesting to see their HR/Personnel file.

Valid requests from individuals for copies of their data under the subject access are processed by the Medical Secretary under the supervision of the Lead GP. The GDPR allows individuals to request information held about them verbally or in writing. In writing can include by paper, electronically to include email and social media. Requests should include what information is required. Sufficient information must be supplied to confirm the identity of the requestor. The request does not have to include the phrase "subject access request" or quote Article 15 of the GDPR, as long as it is clear that the individual is asking for their own personal data.

Requests made on behalf of a patient by a third party

The GDPR allows for requests for personal information to be made via a third party.

The Practice follows the guidelines issued by the ICO therefore, should you receive a request for information from someone other than the patient you should:

- Ensure you are satisfied that the third party making the request is entitled to act on the behalf of the individual. If not the patient should be contacted to confirm a proper informed consent process has taken place. This is particularly important if the request is for the release of copies of a complete patient record to a third party, for example, a solicitor, as the patient will not necessarily know what is contained in their record.

- It is the responsibility of the third party to provide evidence of their permission / authorisation from the patient to act on their behalf – this may be in writing or a power of attorney document

- Special arrangements are made if the Data Subject cannot read or write, is deaf or blind, or cannot speak English or any other languages spoken or understood by the

Practice.

If you believe that the patient may not understand or be aware of what information would be disclosed to the third party making the request on their behalf, you should note this with the request. The Practice may then provide the information directly to the patient rather than to the third party. The patient themselves can then decide whether or not to disclose the information.

Ref: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Concerns re the mental capacity of an individual

As noted by the ICO, "there are no specific provisions in the GDPR, the Mental Capacity Act 2005 or in the Adults with Incapacity (Scotland) Act 2000 enabling a third party to exercise subject access rights on behalf of such an individual."

It is reasonable to assume that an attorney with authority to manage the property and affairs of an individual will have the appropriate authority.

Source: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/