Data Protection, Confidentiality, and Information Security Policy

Policy Statement

Edinburgh GP medical practice processes personal data that relate to employees and patients and is therefore required by law to comply with the General Data Protection Regulations (GDPR), which protects the privacy of individual personal data and ensures that they are processed fairly and lawfully.

The Practice is committed to ensuring that it complies with the GDPR and applies ethical principles to all aspects of its work to protect the interests of employees and patients and maintain the confidentiality and security of any personal data held in any form by the practice. To do this, the Edinburgh GP will comply with the eight data protection principles. In summary, these state that personal data shall be:

- fairly and lawfully processed.
- processed for limited purposes (i.e., obtained only for specified and lawful purposes and further processed only in a compatible manner)
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary.
- processed in line with the individual's rights.
- secure
- not transferred to countries outside the EU without adequate protection

We also recognise the rights of individuals under GDPR:

- The right to be informed.
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing.
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The Practice has developed a GDPR Privacy Notice for Patients and a GDPR Privacy Notice for Staff.

Lawful Basis

We have a legal obligation to hold and record accurate personal health and data records for each of our patients. In accordance with Article 6 paragraph 1(c) of UKGDPR – *"processing is necessary for compliance with a legal obligation to which the controller is subject"*.

The relevant basis in UK law is set out in the Data Protection Act 2018, in schedule 1 condition 2. This condition covers the following purposes:

- preventive or occupational medicine
- the assessment of an employees working capacity
- medical diagnosis
- the provision of health care or treatment
- the provision of social care (this is likely to include social work, personal care and social support services)
- the management of health care systems or services, or social care systems or services

The above is in accordance with Article 9 paragraph 2(h) of UKGDPR.

Responsibilities

This Data Protection, Confidentiality and Information Security Policy applies to all practice employees and any others who have legitimate rights to access and use the practice's information systems.

Compliance with the GDPR and this policy is the responsibility of all practice employees and everyone who has access to practice records. A breach of this policy, whether deliberate or through negligence, could lead to disciplinary action being taken and possible investigation by the General Medical Council. A breach of the GDPR could also lead to criminal prosecution.

The following table lists key responsibilities among the medical team.

Team Member	**Responsibility**
Lead Doctor, Dr David Richardson AND Kirsty Wales, Practice Manager and Data Protection Officer	Data Protection, Confidentiality, and Information Security policy; deals with subject access requests made under the GDPR and requests made under the Freedom of Information Act (Scotland) 2002; training of staff regarding data protection and confidentiality
David Richardson	Data controller (i.e., principal doctor who 'owns' a patient list)
Alanna Merrie	Data controller (i.e., associate doctor who 'owns' a patient list)
Shona Williamson	Data controller (i.e., associate doctor who 'owns' a patient list)
All staff	Compliance with the GDPR and this Data Protection, Confidentiality, and Information Security policy

If you have any questions or comments about processing personal data or this policy, please contact the Practice Manager.

Definition of Personal Data Covered Under the GDPR

The GDPR applies to personal data, which is defined as information which relates to a living individual who can be identified from the information itself or by linking it with other information. This includes an individual's name, address or email address, an online profile or an employee's HR record, sickness absence or appraisal record. There is also 'special category' information which relates to sensitive personal data such as medical information, ethnic origin etc. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

To provide effective care for patients and provide healthcare services, the Practice processes personal data of patients. Personal data means practically any information about, or correspondence relating to, a named individual. It includes both facts (e.g., treatment a patient has had) and opinions (e.g. any concerns the patient or medical team might have about the patient's medical health), including:

- personal information and contact details, including the patient's name, address and date of birth.
- medical, social and medical histories (e.g., past or current medical conditions, current medication, the name of the patient's NHS GP, special needs)
- results of the GP consultation/assessment,
- information about appointments
- any treatments and their costs
- any proposed care, including advice given to the patient and referrals the patient might need.
- any concerns that the patient or medical team might have
- details of the patient's consent for specific procedures (onward referral)
- correspondence with other healthcare workers that relates to the patient's care.

As an employer, the Practice also processes the personal data of employees, including:

- personal information and contact details, including name, address and date of birth.
- health clearance and immunisation status
- employment and educational histories

- absence / leave records
- performance and appraisal information
- information on training and professional development

Procedures for Ensuring Compliance with the GDPR and the Confidentiality and Security of Personal Data

All Staff including associate Doctors.

To maintain a good patient–medical team relationship, it is essential that patients feel they can provide personal information to medical team members with the knowledge that this information will be kept securely and not shared unlawfully. It is also important that patients are able to provide, in confidence, full details of their medical, social and medical histories to facilitate safe and effective care. To achieve this, all staff must follow the procedures listed below.

- Comply with the 8 data protection principles and the General Medical Council principles set out in the 'Professional Standards for Doctors'.
- Undergo training in processing personal data and confidentiality.
- Keep any personal data or confidential data that they hold, whether in electronic or paper format, securely, which includes:
    - storing paper files with personal data in lockable filing cabinets that are locked when authorised staff are not present to monitor access.
    - storing electronic files containing personal data on password-protected computer systems
    - 'Screen-locking' unattended computers, all workstations will automatically lock after 2 minutes if not used.
    - not sharing computer passwords with unauthorised people, not writing down passwords and not keeping passwords on or near their computer
    - not forwarding emails containing personal data to internet email accounts as these are not secure.

- holding personal data on laptops only where there is a clear business necessity and permission is sought from the Practice Manager (if there is a necessity, ensure it is fully encrypted)
- avoiding carrying personal data on removable media (e.g., memory sticks)
- not using unlicensed software on Practice computers
- ensuring windows and doors are secured if you are the last to leave the practice.

- Practice good record-keeping, and ensure records are:
  - accurate
  - dated
  - contemporaneous
  - comprehensive
  - secure
  - legible and written in language that can be read and understood by others and is not derogatory.
- Maintain the confidentiality of any personal data by, for example:
  - ensuring that personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party (e.g. avoid working on personal data such as application forms on public transport, do not discuss identifiable information about patients with anyone outside the practice, including friends, family and schools, or leave messages about a patient's care with an unauthorised third party or on an answering machine) (NB: this also applies after termination of employment)
  - respecting patient privacy for discussions of a sensitive nature (e.g., discussion of medical information, payment, or asking patients for proof of exemption status)
  - using personal data only for the purposes for which they are authorised in the relevant Data Protection registration.

- Ensure patients know what information is to be shared, why it is being shared and the likely consequences of sharing (or not sharing) the information and give patients the opportunity to withhold permission to share their information.
- Share personal data only on a 'need to know' basis and following consent from the patient; for example:
    - to another health professional for the provision of effective care and/or treatment
    - to a laboratory for the processing of test samples
- Check that any personal information that you provide in connection with your employment is accurate and up to date and inform the Practice Manager of any changes to this information.
- Inform the Practice Manager/Data Protection Officer, who is responsible for ensuring compliance with the GDPR and this policy, of any suspected or actual breach of the GDPR or this policy.

Data Controllers

Data controllers are those who hold personal records (e.g., doctors who are the 'owner' of their own patient list). All data controllers must follow the procedures detailed above for staff, and the procedures listed below.

- Register with the UK Information Commissioner
- Keep the details of the registration up to date and renew this registration annually.

General Medical Practice

All staff contracts and agreements include a clause regarding confidentiality of personal data.

- Keys for lockable storage cabinets are held only by medical team members who require regular access to the information they contain. Keys are stored in a safe place/secure key cabinet which is secured to the wall in the reception cupboard.
- Practice workstations have a full audit trail facility to prevent deletion or overwriting of data.

- All workstations are password protected and access to patient software systems is by MFA.
- IT administrator applies ‘Password Policy’ that requires change every 3 months.
- Each computer is fitted with anti-virus software.
- Back-ups of the Practice’s patient software records are made regularly throughout the day as our system is cloud based, (back-up is made to Amazon based servers located at various locations in the UK) and this allows for quick retrieval of information.
- Back-ups are tested by our IT provider to ensure data can be retrieved in a useable format.
- Adult patient records are kept for life and 3 years after death.
- Personal data are reviewed, updated, and deleted in a confidential and secure manner when no longer required.
- Windows are fitted with locks and the practice is fitted with an intruder alarm that is set each night to increase security.
- A continuity plan that includes procedures for protecting and restoring personal data is in place in the event of a major incident.

Sharing Personal Information

To provide patients with appropriate care, we might need to share personal data with:

- another health professional who is caring for the patient
- the patient’s NHS GP
- a medical laboratory
- a private health / medical scheme if the patient is a member.

To fulfil our duties as employers, we might need to share staff personal data with:

- other employers
- the Inland Revenue
- pension providers
- educational institutions

- regulatory and professional bodies

In these cases, only the minimum information required will be shared.

Disclosure Without Consent

Exceptional circumstances might override the duty to maintain confidentiality. Where possible, we will inform the patient or staff member of requests to share personal information. The decision to disclose information must only be taken by senior staff. Examples include:

- situations where there is a serious public health risk or risk of harm to other individuals.
- when information is required by the police to prevent or detect crime or to apprehend or prosecute offenders (if not providing the information would prejudice these purposes)
- in response to a court order
- to enable a doctor to pursue a legal claim against a patient.

Dr David Richardson is responsible for making the decision regarding whether personal data should be disclosed.

Data Breaches

We will always aim to ensure that the information we hold is held securely. We will report any detected data breaches that are likely to result in a risk to the rights and freedoms of the individuals affected to the ICO within 72 hours of becoming aware of them. We will also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms. We will also inform the ICO of any breach of confidentiality.

We will document all data breaches, even those that are not notifiable to the ICO, and will include information on the steps taken to mitigate any adverse effects and to ensure that the breach does not reoccur.

Data Subject Rights

We recognise the rights of individuals under GDPR, and we have processes in place to deal with relevant requests. We provide a Privacy Notice to comply with an individual's right to be informed.

Where an individual requests access to their information, we will provide this free of charge, and in an electronic and commonly used format within one month of the request, unless we deem the request to be unreasonable or excessive. If we refuse a request for access, we will inform the individual of our decision, and the reasons for it, within one month of their request. We will also inform the individual that they have the right to appeal to the ICO and to seek legal advice.

Where an individual notifies us that the information, we hold about them is incorrect, we will rectify this. Where an individual asks us to delete their information, we will consider this based on the type of information and any legal or professional obligations to retain the data. Where we cannot delete the information, we will inform the individual of this within one month of their request. Where an individual asks us to transfer their information to another medical practice, we will ensure that this is done in a confidential and secure manner. Individuals also have the right to object to data processing or to ask for this to be restricted.

We do not use personally identifiable information in automated decision making or data profiling.