Fochabers
Medical Practice

Data Protection Policy

The Practice is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) and all other data protection legislation currently in force. The Regulation applies to anyone processing personal data and sets out principles which should be followed and gives rights to those whose data is being processed.

To this end, the Practice endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

- processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency')
- processed no further than the legitimate purposes for which that data was collected ('purpose limitation')
- limited to what is necessary in relation to the purpose ('data minimisation')
- accurate and kept up to date ('accuracy')
- kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation')
- processed in a manner that ensures security of that personal data ('integrity and confidentiality')
- processed by a controller who can demonstrate compliance with the principles ('accountability')

These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the Practice will:

- observe fully the conditions regarding having a lawful basis to process personal information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements
- ensure the information held is accurate and up-to-date
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)

Keith J Anderson MBE | Practice Manager | 12 High Street | Fochabers | IV32 7EP | 01343 820247

- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection
- Have a continual Security Improvement Plan
- Keep internal records of data processing activities
- Use Data Protection Impact Assessments where appropriate.

GDPR and General Practice

The main reason for GPs processing is necessity for medical purposes, but there are others e.g. legitimate interest, vital interest, legal obligation, consent etc.

Medical Purposes

Information will be processes by a health professional (or equivalent duty of confidentiality). This includes preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services. The Practice will document decisions taken about processing activity.

Rights for Individuals

Patients have:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure[1]*
- 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 will record:

- Name and details of your organisation, your representative and data protection officer (+partners & data processors)
- Purposes of the processing.
- Description of the categories of individuals and personal data.
- Categories of recipients of personal data.

[1] *The Right to Erasure and the right to object equates to the right to be forgotten

Keith J Anderson MBE | Practice Manager|12 High Street | Fochabers | IV32 7EP | 01343 820247

- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.
- Contracts with data processors, information sharing activities and any relevant agreements
- Records of controversial decisions (e.g. prejudice tests, privacy assessments, etc.)

Notice for Patients Regarding Research Data Collection

The staff at the Practice record information about patients and their health so that they can receive the right care and treatment. The Practice needs to record this information, together with the details of the care required so that it is available each time the patient requires treatment.

The information recorded about patients may be used for reasons other than personal care; for example to help protect the health of the general public, planning for the future, training of staff, and to carry out medical and other health research.

The Practice is involved in research studies which require access to anonymous information from patients' notes. Patients cannot be identified from these notes as all personal details: name, address, postcode, and full date of birth are removed. Individual patients' records are added into a much larger anonymous database from many patients across the UK, which is used by researchers outside of this practice.

Patients wishing to opt out of this data collection scheme should let the Practice know. Patients who choose to opt out of the data collection programme can be assured that no data from their records will be collected or used in any research; and their care will not be affected in any way.

If anything to do with research would require patients to provide additional information about themselves, they will be contacted by a GP to check if they are willing to take part. They will not be identified in any published results.

Patients have a right of access to their health records. If at any time they would like to know more, or have any concerns about how the Practice uses patient information they can contact the Practice Manager in the first instance.

Everyone working for the NHS has a legal duty to keep the information about you confidential

Obligation to report data breaches

The Practice, and its employees, have a duty to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify the Practice Manager who will, in turn, contact those concerned directly.

Employees Personal Information

Throughout employment and for as long as is necessary after the termination of employment, the Practice will need to process data about you. The kind of data that the Practice will process includes:

- any references obtained during recruitment
- details of terms of employment
- payroll details
- tax and national insurance information
- details of job duties
- details of health and sickness absence records
- details of holiday records
- information about performance
- details of any disciplinary and grievance investigations and proceedings
- training records
- contact names and addresses
- correspondence with the Practice and other information that you have given the Practice

The Practice believes that those records used are consistent with the employment relationship between the Practice and yourself and with the data protection principles. The data the Practice holds will be for management and administrative use only but the Practice may, from time to time, need to disclose some data it holds about you to relevant third parties (e.g. where legally obliged to do so by HM Revenue & Customs, where requested to do so by yourself for the purpose of giving a reference or in relation to maintenance support and/or the hosting of data in relation to the provision of insurance).

In some cases the Practice may hold sensitive data, which is defined by the legislation as special categories of personal data, about you. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet the Practice's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of which may cause concern or distress, you will be asked to give express consent for this information to be processed, unless the Practice has a specific legal requirement to process such data.

Access to Data

You may, within a period of one month of a written request, inspect and/or have a copy, subject to the requirements of the legislation, of information in your own personnel file and/or other specified personal data and, if necessary, require corrections should such records be faulty. If you wish to do so you must make a written request to your Practice Manager. The Practice is entitled to change the above provisions at any time at its discretion.

Data Security

You are responsible for ensuring that any personal data that you hold and/or process as part of your job role is stored securely.

You must ensure that personal information is not disclosed either orally or in writing, or via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

You should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and where possible it should be locked away out of sight i.e. in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight i.e. in the boot of a car.

Keith J Anderson MBE | Practice Manager|12 High Street | Fochabers | IV32 7EP | 01343 820247