**General Data Protection Regulation**

The General Data Protection Regulation (GDPR) is a new law that determines how your personal data is processed and kept safe, and the legal rights that you have in relation to your own data.

GDPR regulations apply from the 25th May 2018, and will apply even after the UK leaves the EU.

What GDPR will mean for Patients

GDPR sets out key principles about processing personal data:

1. Data must be processed lawfully, fairly and transparently
2. It must be collected for specific, explicit and legitimate purposes
3. It must be limited to what is necessary for the purposes for which it is processed
4. Information must be accurate and kept up to date
5. Data must be held securely
6. It can only be retained for as long as is necessary for the reasons it was collected

There are also stronger rights for patients regarding the information that Practices hold about them. These include:

1. Being informed about how their data is used
2. Having access to their own data
3. Ask to have incorrect information changed
4. Restrict how their data is used
5. Move their patient data from one health organisation to another
6. The right to object to their patient information being processed (in certain circumstances

**What is GDPR?**

GDPR stands for General Data Protection Regulation and is a piece of legislation introduced in May 2018 along with the Data Protection Act 2018 sets the regulation about how organsiations must handle information in the UK. GDPR applies to the UK and EU; it covers anywhere in the world in which data about EU citizens is processed.

GDPR has strengthened many of the principles of the previous UK leglisation known as the Data Protection Act 1998. The main changes are:

• Practices must comply with subject access requests within one calander month

• Where we need your consent to process data, this consent must be freely given, specific, informed and unambiguous

• There are new, special protections for patient data

• The Information Commissioner’s Office must be notified within 72 hours of a data breach

• Higher fines for data breaches

What is consent?

Consent is permission from a patient – an individual’s consent is defined as “any freely given specific and informed indication of a patient’s wishes by which the data subject signifies their agreement to personal data relating to them being processed.”

To protect your right to privacy, and we may ask you to provide consent to do certain things, for example completing a medical report. Individuals also have the right to withdraw their consent at any time.