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.

The regulation applies from 25 May 2018, and will apply even after the UK leaves the EU.

What GDPR will mean for patients

The GDPR sets out the key principles about processing personal data, for staff or patients;

- Data must be processed lawfully, fairly and transparently
- It must be collected for specific, explicit and legitimate purposes
- It must be limited to what is necessary for the purposes for which it is processed
- Information must be accurate and kept up to date
- Data must be held securely
- 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;

- Being informed about how their data is used
- Patients to have access to their own data
- Patients can ask to have incorrect information changed
- Restrict how their data is used
- Move their patient data from one health organisation to another
- The right to object to their patient information being processed (in certain circumstances)

Fairfield Medical Centre

What is GDPR?

GDPR stands for General Data Protection Regulations and is a new piece of legislation that will supersede the Data Protection Act. It will not only apply to the UK and EU; it covers anywhere in the world in which data about EU citizens is processed.

The GDPR is similar to the Data Protection Act (DPA) 1998 (which the practice already complies with), but strengthens many of the DPA's principles. The main changes are:

- Practices must comply with subject access requests
- Where we needs 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 – up to 20 million euros