MAYNARD COURT SURGERY

GDPR

**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** comes into force on 25 May 2018 and even though the UK is due to leave Europe in the next 12 months, it will still apply to all businesses handling EU residents' data, effectively replacing the Data Protection Act 1998.

'Controllers' and 'processors' of data need to abide by the **GDPR**. A data controller states how and why personal data is processed, while a processor is the party doing the actual processing of the data. So the controller could be any organisation, from a profit-seeking company to a charity or government. A processor could be an IT firm doing the actual data processing.

It's the controller's responsibility to ensure their processor abides by data protection law and processors must themselves abide by rules to maintain records of their processing activities. If processors are involved in a data breach, they are far more liable under **GDPR** than they were under the Data Protection Act.

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 ‘SAR’ - subject access requests.

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 up to 20 million euros.

**What is patient data?**

Patient data is information that relates to a single person, such as his/her diagnosis, name, age, earlier medical history etc.

**What is consent?**

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

The changes in **GDPR** mean that we must get explicit permission from patients when using their data. This is to protect your right to privacy, and we may ask you to provide consent to do certain things, like contact you or record certain information about you for your clinical records. Individuals also have the right to withdraw their consent at any time.