**GDPR, Data Extraction/Data Sharing, and your right to object**

General Data Protection Regulations (GDPR) come into force in May 2018. Basically these cover much the same ground as Information Governance, but they lay more emphasis on written policies and procedures, and on organisations such as surgeries taking responsibility for informing staff and patients of the data they hold and how it is managed. Most of the data we hold about our patients is on our clinical computer system (EMIS Web), which is managed from a remote server at EMIS headquarters in Leeds. Patients should be aware that this data (and in fact all computerised GP records in doctors' surgeries across the UK) is regularly accessed by a data extraction service called the General Practice Extraction Service (GPES), but that this service only extracts anonymised data for the sake of national statistics about patients and their health (for example the National Diabetes Audit).

Some non-anonymised, personal data for individual patients is also routinely shared with the national Summary Care Record service, which allows other health professionals to see things like your allergies and repeat prescriptions: this information can be very helpful if you have to be admitted to hospital as an emergency. There may also be instances where we ask permission to share your personal details with other health services - for example if we have a Care Plan for an elderly or vulnerable patient, including next-of-kin details and emergency contact telephone numbers, we might ask your permission to share it with the out-of-hours services and the ambulance service, so that they would have access to the information if something happened when the surgery was closed. You are entitled to refuse permission for any of these data extractions or data sharing arrangements: if you do so then your decision will be recorded on your notes and the data extractions and data sharing will not take place for you.