Summary
The Data Protection Act 2018 will align with GDPR. This new regulation/legislation has been introduced to strengthen data protection for individuals within the EU and will come into force from 25th May 2018. The Practice Policies and documentation around Information Governance and Data Protection is associated to the UK Data Protection Act 2018 and as such documentation will be updated following a review of the new published Act in line with GDPR.

Accountability
We must demonstrate how we comply with the Data Protection Act 2018/GDPR – so it's important to complete data flows as this will identify any risks in sharing or transferring data.

Data Breaches & Fines
All serious breaches must be reported to the Information Commissioners Office within 72 hours by your appointed Data Protection Officer (DPO).

The Information Commissioner can fine organisations up to €20 million or 4% of annual global turnover for serious data breaches.

Privacy Notices
All Fair Processing Notices previously used by NHS Organisations have to be replaced with a Privacy Notice on-line and in leaflet form for Patients, Children, Staff, and Charities

Subject Access Requests
Must now be completed within a month and are free of charge

Data Protection Impact Assessments
Previously called Privacy Impact Assessments MUST be used for all changes in systems and process to identify risks. These documents have to be approved by your organisations Data Protection Officer

The new General Data Protection Regulation (GDPR) & the Data Protection Act 2018 (DPA18) replace the Data Protection Act 1998

25th May 2018

What you need to know!
ICO GDPR Link

Personal Data
This is any data about an individual that could identify them. The definition of personal data is expanded under GDPR to include NHS Numbers and Hospital numbers – for the purpose of secondary use – we **MUST** anonymise / pseudonymise data.

Consent
Despite a lot of mis-communication from online companies – health care providers **DO NOT** have to ask for consent to process health care information. This falls under another legal basis within GDPR.

Data Controllers
Must register with the Information Commissioner's Office annually to register what information they manage and ensure all contractual arrangements are in place with staff and 3rd parties. A Data Controller can be fined for a serious breach.

Data Protection Officer
This is a new role that **ALL** Data Controllers must have in place.

It is the responsibility of your General Practice to ensure that you have sufficient resources for this role.

Individuals' Rights
Individuals have increased rights under the Data Protection Act 2018/GDPR for example the 'right to be forgotten' however this only applies in certain circumstances such as marketing, or situations where consent is necessary for processing. Consent is not required for processing healthcare data. Our patients have the right however to rectify any data we hold on them that is incorrect.

Data Processors
Provide processing services to Data Controllers and must have contracts in place to provide such services. Data Processors under GDPR can now also be fined by the Information Commissioner's Office for a serious data breach.