GDPR Headlines - Top Tips

What is the GDPR (General Data Protection Regulation)?

The GDPR is a regulation that will become applicable from 25th May 2018. Its intention is to strengthen data protection for individuals across the European Union. The Data Protection Bill will become law when enacted as the Data Protection Act 2017 and will bring provisions of the GDPR in to UK law and establish continuity of the GDPR in the UK post Brexit. The Data Protection Act 1998 will be repealed.

Compliance is essential as fines under the GDPR are up to a maximum of 20 million Euro or 4% of turnover.

The GDPR strengthens the controls that organisations (data controllers) are required to have in place over the processing of personal data, including pseudonymised data.

Headline Requirements

- Mandatory appointment of a Data Protection Officer (DPO) for all public authorities
- An obligation to demonstrate compliance with the new law
- Legal requirements for security breach notification
- Removal of charges (in most cases) for providing copies of records to patients or staff who request them
- Requirement to keep records of data processing activities
- Data Protection Impact Assessments required for high risk processing (including the large-scale processing of health-related personal data)
- Data protection issues must be addressed in all information processes
- Specific requirements for transparency and fair processing
- Tighter rules where consent is the basis for processing

Practices that are performing well in their information governance toolkit will have a good baseline to work from. However, organisations will be required to take specific actions and to be able to evidence that they have done so.

The Information Governance Alliance (see: https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance) has indicated that they'll publish resources

for primary care in March/April and we also know that the General Practitioners' Committee is in the processing of drawing up guidance for practices which will be published shortly.

In the meantime, the Information Commissioner's Office has published a couple of checklists which may be helpful:

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

And the GPC has advised the following:

- Practices should already have data protection policies and procedures in place; under the GPDR they will need to be able to show that they are written down and accessible to staff and that staff are aware these policies are in place.
- Practices should already know what personal data they hold, who can access them (and why), with whom the data is shared (and the legal basis for this), and what security measures are in place for storing and sharing; under the GPDR it will be a requirement to have an audit/record to state the above, which can be provided to the ICO upon request (e.g. if there is a complaint from a patient about a breach or non-compliance).
- Practices should already have 'fair processing' or 'privacy notices' displayed in the practice and on the practice website. These notices should explain to patients how their data might be used, when they might be shared and with whom and any rights of objection.
- Practices need to be able to demonstrate their compliance with the regulations upon request – at present they just need to be compliant; under GPDR they will need to be able to demonstrate that they have all policies and procedures in place, as well as a record of the above. Essentially if the ICO turns up at a practice, they need to be able to provide them with a document showing all of the above.
- Penalties for data breaches, including not being compliant and not being able to demonstrate compliance are much higher under the GDPR, and have lower thresholds (i.e. you can be fined more for a lesser offence).
- Practices will no longer be able to charge a fee for patients to access their own information.
- Practices which are already compliant with the Data Protection Act 1998 will be in a strong position for the introduction of the GDPR. The BMA has existing guidance on GPs as data controllers under the DPA: which you can read here .

The LMC will be sending out further information and advice to practices as it becomes available and we hope the above is helpful in the meantime.