What is GDPR, and why is it important?

Kensington Group Practice
DONEGALL ROAD AND FINAGHY
Medical Centre

The General Data Protection Regulation replaces the existing data protection laws from May 2018 - this is a summary of what the changes will mean.

The UK's existing data protection laws came into effect over 20 years ago, and there have been big changes in technology, access and the use of data since they came into effect. Recent data security advancements also mean that there is a higher risk of personal information being illegally accessed and it is up to organisations that hold patient data to protect it so that it is safe from theft and misuse.

This means that the existing laws have been reviewed and are now being updated and enhanced to protect the data and improve the way that organisations store patient information.

What is GDPR?

The new General Data Protection Regulations (GDPR) will come into force on 25th May 2018 and will ensure that companies protect information, but also improve the rights of people to access the information that companies hold about them.

What are the key changes from before?

There are bigger fines for companies that do not follow the rules. Under the current Data Protection Act, the maximum fine is £0.5million. The new GDPR fines are up to 20 million Euros or up to 4% of a company's annual turnover – whichever is bigger.

People who process the data ('Data Processors') are also accountable for the data they have access to – they must follow rules for storing patient data, processing and notifying their Data Controllers when anything untoward has happened to that information (a 'data breach')

Every organisation has to carry out a data 'privacy impact assessment' when they implement any new processes or use new systems. This means that they must check if there is a risk to data security, and act to make sure it has been dealt with.

GDPR also requires practices to ensure they have patient permission (or 'Consent')to use the data about them. This consent must be freely given, specific, informed, clear about what their data is used for and specify that the patient has given consent to their data being processed. This means that consent can't be inferred by a patient's silence, pre-ticking boxes or if patients do not respond, or their inactivity.

Patients can access their data by making a Subject Access Request – practices must respond within 1 month from the date they received the request. Practices will provide the requested information free of charge except in specific circumstances, such as if the requests are manifestly unfounded, excessive or if it is a request for further copies.

There is a ‘Right to be forgotten’, which means that patients have the right to request that the practice deletes personal data about them, but only in certain circumstances;

The data is no longer needed

Patient withdraws their consent

Patient objects to processing and there is no compelling reason that overrides their interests.

There is also the ‘right to portability’ – the ability to have their personal data moved from one controller to another, and it to be done in a safe and secure manner.

What is a ‘Data Breach’?

A Data Breach is when personal data about an individual has been accessed or distributed without authorisation. It may mean that someone gets unauthorised access to data, but it can also happen if there is unauthorised access within an organisation, or if someone accidentally changes or deletes personal data.

Under GDPR, if there is a risk to people’s rights and freedoms then it must be reported to the relevant authority – if there is a high risk to people’s rights and freedoms, then they will also need to notify the individuals who have been affected.

Health data has particular protections under the GDPR to protect vulnerable patients – it has additional restrictions about how and when it can be processed, and the level of consent required to authorise the processing.

Useful Links

Information Commissioner's Office : https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/