CARNARVON MEDICAL CENTRE

GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR is replacing the Data Protection Act (DPA) 1998 and will apply in the UK from 25th May 2018.

What is the GDPR?
The General Data Protection Regulation (GDPR) is an EU Regulation, developed to update data protection law and to unify all EU Member States (Countries) approach to data protection and ensure the law is applied identically in every EU Country.

Who must comply with the GDPR?
The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the DPA – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. GDPR applies to 'controllers' and 'processors' that process the data of EU citizens regardless of where in the world the actual 'processing' takes place.

Further reading in the GDPR
(See Articles 3, 28-31 and Recitals 22-25, 81-82)
What information does the GDPR apply to?
Personal data
Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier e.g. an IP address, genetic and biometric data e.g. finger prints, and DNA etc. can be personal data.

Sensitive personal data
The GDPR refers to sensitive personal data as 'special categories' of personal data. These categories are broadly the same as those in the DPA, and require additional conditions to process lawfully. For example health data is classed as special category data- basically; it's anything that could cause harm to an individual or their reputation.

Further reading in the GDPR
(See Articles 2, 4, 9, 10 and Recitals 1, 2, 26, 51)
Key areas to consider:
Lawful processing
For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data. This needs to be communicated to Data Subjects through a Privacy Notice in an effort to be transparent.

Further reading in the GDPR
(See Articles 6-10 and Recitals 38, 40-50, 59)

Consent

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity.

Further reading in the GDPR
(See Articles 4(11), 6(1)(a), 7, 8, 9(2)(a) and Recitals 32, 38, 40, 42, 43, 51, 59, 171)

Children's Personal Data

The GDPR contains new provisions intended to enhance the protection of children's personal data. The GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 can't give that consent themselves (unless they are deemed to have sufficient capacity to consent for themselves from the age of 13 years old in the UK) and instead consent is required from a person holding 'parental responsibility'.

Further reading in the GDPR
(See Article 8 and Recitals 38, 58, 71).

Individual's rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA.

The GDPR provides the following rights for Individuals:

- The right to be informed
- The right to be informed encompasses the obligation to provide a Privacy Notice. It emphasises the need for transparency over how personal data is used.

Further reading in the GDPR
(See Articles 12(1), 12(5), 12(7), 13, 14 and Recitals 58-62)

The right of access (Subject Access Requests)

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

A copy of the information must be provided free of charge.

There will be less time in which to comply with a subject access request under the GDPR. Information should be provided within one month of receipt of the request.

Further reading in the GDPR
(See Articles 12, 15 and Recital 63)

The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Certain exemptions apply to health related data and when it may be rectified.

Further reading in the GDPR
(See Articles 12, 16 and 19)

The right to erasure (the right to be forgotten)

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Again, certain exemptions apply.

Further reading in the GDPR
(See Articles 17, 19 and Recitals 65 and 66)

The right to restrict processing

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar. When processing is restricted, the personal data may continue to be stored, but not further processed.

Further reading in the GDPR
(See Articles 18, 19 and Recital 67)

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

Further reading in the GDPR
(See Articles 12, 20 and Recital 68)

The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Further reading in the GDPR
(See Articles 12, 21 and Recitals 69, 70)

Rights related to automated decision making and profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

Further reading in the GDPR
(See Articles 4(4), 9, 222 and Recitals 71, 72)

Accountability and Governance

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

Further reading in the GDPR
(See Article 30, Recital 82)

Data Protection by Design and by Default

Under the GDPR, technical and organisational measures must be taken to show that data protection rules have been considered and integrated into processing activities.

Further reading in the GDPR
(See Article 25 and Recital 78)

Data Protection Impact Assessments

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to

identify risks associated with new projects, processes and systems and where possible fix problems and mitigate against risks at an early stage.

Further reading in the GDPR
(See Articles 35, 36, 83 and Recitals 84, 89-96)

Appointing a Data Protection Officer

Under the GDPR, a Data Protection Officer must be appointed if the organisation:

- is a public authority (except for courts acting in their judicial capacity);
- carries out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Contact details for the Data Protection Officer can be found in the Privacy Notice.

Further reading in the GDPR
(See Articles 37-39, 83 and Recital 97)

Data Breach Notification

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected within 72 hours of becoming aware of the breach.

Further reading in the GDPR
(See Articles 33, 34, 83 and Recitals 85, 87, 88)

Transfers of Data to Third Countries or International Organisations

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Further reading in the GDPR
(See Article 45 and Recitals 103-107, 169