General Data Protection Regulation (GDPR)

What Is GDPR?

The GDPR (General Data Protection Regulation) is a set of requirements for the protection of personal data that comes into force from the 25th May 2018.

It will replace the Data Protection Act in the UK and covers much of the same ground. However, it does expand on the previous Act and includes, or at least formalises, extra provision which is predominately aimed at curbing the current abuse of our personal data.

Principles

The GDPR is being introduced by the European Union member states, of which we are still one, to standardise data protection and usage guidelines throughout the EU.

It is designed to replace and update the individual countries' data protection regulations for our modern and data orientated world.

Much of the new regulations focus is to address larger multi-national companies and their handling and storing of data eg Google, Facebook, Amazon etc.

For small and medium businesses little will actually change in day to day activities, it will simply be formalised and tightened up.

Key Details

a) Who does it apply to?

The short answer is everyone. Everyone who stores or manipulates personal data, outside of home or personal usage, is required to comply, to the best of their ability, with the GDPR when it comes into force.

There are two broad classifications of businesses define by the GDPR, Controllers and Processors.

Controllers are defined as the collectors of the data, the entity that holds it, this means you, you are the controller of the patient data stored within your system.

Processors are defined as those who use the information provided by the controller, an example would be a company performing a mailshot for the practice.

b) What information does the GDPR relate to?

There are two classes of data to which the GDPR applies, Personal data and Sensitive Personal data.

Personal data is defined as any information that can be used to directly or indirectly identify a person eg name, address, date of birth etc but also includes data like phone numbers and email addresses.

Sensitive Personal data covers such data as genetic, biometric and medical information. This would include patient prescriptions and other ocular health information.

Lawful basis for processing

This means, what allows you to use personal data within your business?

There are a number of different bases for processing that have be codified in the GDPR, only three, arguably two, are really relevant for yourselves.

Special Category Data – This classification covers a number of particular types of data, one of which is medical data, or data relevant to healthcare. This provision covers usage of personal data for the patient's best interests eg ensuring regular check-ups, referral to other health professionals etc.

Legitimate Interest – This is a broader and, somewhat, more flexible basis for the use of personal information. It could relate, for example, to using your patient data for a promotional mailshot, so long as it is relevant to the primary operations of the business.

Consent – This basis for data use is the one which is well known to be abused under the existing Act eg pre-ticked boxes on websites. Therefore, the GDPR has set very strict standards attached to this category, but you don't need it, as any use of your patients' data should fall within the provisions of Special Category or Legitimate Interest.

Individual Rights

The GDPR outlines a number of specific rights that a person has with regards to the data you may hold on them.

a) **Right to be informed** – This provision covers the person's right to be informed what information is being held, for what purpose and for how long that information is held. This can be fulfilled by either explaining it verbally or via a standard Optisoft document to all new patients.

b) **Right of access** – This provision covers the person's right to a copy of information held, either in a printed or electronic format. Within Optisoft this requirement can be fulfilled with the use of a standard document, including the relevant merge codes that can be printed or sent electronically on request.

c) **Right to rectification** – This provision covers the individual's right to have their data rectified, or corrected, if it is incorrect or incomplete. Should this happen, which is unlikely, it can be fulfilled by simply editing their record in Optisoft.

d) **Right to erasure** – This covers the individual's right to have their data removed from your systems. This can be fulfilled in Optisoft by deleting the patient record, which removes the data from the system.

However, as you will be aware, the GOS Terms of Service requires you to keep all records including voucher audit trails for 7 years. NHS Guidelines state "*the recommended retention period of records is 10 years following the patient's last visit. In the case of children, the recommended retention period of records is until the patient's 26th birthday. Even where a patient has died, their records should be kept for 10 years following the death*." Therefore, before deleting any electronic records it is recommended that hard copies are printed and stored. Full clinical audit trails can be printed from OptomNotes and all other dispensing records can be printed individually.

e) **Right to restricted processing** – This covers the individual's right to prevent you from processing their personal data, but still wish for you to retain the data. This can be fulfilled in Optisoft by the use of an Analysis Code used as criteria to prevent their data being exported for marketing purposes and by ensuring that all their recall categories are purely health related.

f) **Right to data portability** – This relates to the individual's right to a digital copy of their data that they could then use themselves or take to another practice. This can be fulfilled in Optisoft by exporting their data via the Report Generator and provided them with a comma separated value (CSV) file. In reality,

they won't be able to do anything with it currently, as there is no standard data format agreed between the PMS suppliers, but there probably will be in the long-term.

g) **Right to object** – This concerns the individual's rights to object to the processing for the purposes of marketing, research and profiling. This means that they can opt out of their data being processed as a basis for research, for example, and you can fulfil this in Optisoft by the use of Analysis Codes as above.

h) **Rights related to profiling** – These rights cover the automated profiling and decision making based on individual's data. This is one of the rights relating the usage of data by larger entities we mentioned earlier and is very unlikely to have any bearing when related to your data within the Optisoft system.

Security

The GDPR also covers the requirement for security of personal data and some areas that may need to be addressed within your practice are listed below:

a) **Unsupported Systems** – Windows XP is no longer supported by Microsoft, for example, and as such this means that it is now classed as insecure. Microsoft no longer release security updates and fixes for Windows XP so any vulnerabilities will not be addressed, therefore PCs running XP should be replaced or upgraded. If this is not possible then measures should be taken to minimise the risk, such as isolating the PC by disabling internet access on that PC eg legacy imaging systems, diabetic screening etc.

b) **Backups** – Any backups, whether within the practice or at an external location, need to be secure and inaccessible to third parties. The easiest way to achieve this is by ensuring that the backup is encrypted and we do this as standard with the Optisoft backup solution.

c) **Unattended PCs** – Efforts should be made to ensure that patient data is not accessible to unauthorised persons eg PCs should be locked when unattended to prevent access.

Accountability and Governance

The aim of GDPR is to minimise the risk of personal data being misused or used by unauthorised parties, it provides a framework for business to work to in order to meet this end.

The GDPR requires that measures are put in place within the business to comply with its provisions to the best of your ability.

Optisoft would recommend that you use this document as a foundation to detail both your data processing activities and how you will fulfil your obligations under GDPR.

Supplier Certification

As part of the guidance for implementing the new data security and protection requirements, The LOCU/OC states that IT suppliers must have one of the appropriate certifications from the following:

- ISO/IEC 27001:2013 certification
- Cyber Essentials (CE) certification
- Cyber Essentials Plus (CE+) certification
- Digital Marketplace

Optisoft has Cyber Essentials (CE) certification in place.

Further reading

If you would like to know more, the best place to start would be here and we have organised our information in the same format to make that easy for you.

Disclaimer

The above is based on our understanding of GDPR, but we are not lawyers and nothing in this document should be taken as being legal advice.