EASAPS

GDPR

Surgeons Guide

May 2018

The General Data Protection Regulation

GDPR is the revision to the European Union's Data Protection Directive (1995) and is seen as having far reaching implications due to an extended territorial scope, and commitment to Data Subject rights. GDPR becomes law throughout the EU on the 25th of May 2018.

GDPR focuses on personal information. Information that is specifically relevant to an individual, referred to as the "Data Subject" in the regulation.

GDPR affects any organization, located anywhere in the world that collects data and is subject to the scope of the regulation.

GDPR not only applies to organizations located within the EU but it will also apply to organizations located outside of the EU if you process personal information (PI). It applies to all surgeons/hospitals/clinics processing and holding personal data of data subjects (patients/clients etc.) residing in the European Union, regardless of your location.

Roles

An important aspect of GDPR is to understand the roles, and the obligations of those roles as defined by the regulation. The regulation refers to information as data, and categorizes the roles as follows:

The Data Subject

The individual to whom the personal data refers, e.g. a patient, or client.

The Data Processor

Any staff member who processes the personal data on behalf of the data controller, e.g. a Surgeon/Doctor/Ward sister/Nurse or any other clinical admin staff.

The Data Controller

The person, or persons who determine the purpose and the way personal data is to be processed, at the hospital/clinic or surgery. (A person must be identified within your organisation to act as Data Controller.)

Simple Guidelines for doctors

1. Know what you have and why you have it
2. Manage data in a structured way
3. Ensure you have consent and make sure that it is evidenced
4. What medium is the data stored on (Paper/Hard Drive/USB stick)
5. Encrypt what **you** wouldn't want to be disclosed (encryption)
6. Design a security aware culture, store data securely
7. Know who is responsible for it (Data Controller)
8. Be prepared – expect the best but prepare for the worst (Breach control)

Personal Data Classification

It is important to understand where personal information is held, and that the Data Controller understands how the data is to be used. This is helped by understanding personal data classification as follows:

Personal Data

Means data which relates to a living individual who can be identified;

From the data, e.g. birth date combined with last four digits of National Insurance or other social security type number and name, credit card numbers with cardholder name, Tax ID or other identification card with name etc.

From the data and other information which is in the possession of or is likely to come into the possession of the data controller.

Sensitive Personal Data

Sensitive Personal Data refers to information that is likely to cause emotional, in addition to possible physical harm, and consisting of information as to:

- The racial or ethnic origin of the data subject.
- The data subject's political opinions.
- The data subject's religious beliefs or other beliefs of a similar nature.
- Whether the data subject's is a member of a trade union or association.
- Their physical or mental health, medical conditions or history.
- The data subject's sexual life.
- The data subject's commission or alleged commission by him of any offence.
- Any proceedings for any offence committed or alleged to have been committed.

Scope

GDPR provides clarity of responsibility and of commitment to the rights of the individual to whom the personal information belongs. GDPR clarifies relevance, particularly that a Data Controller never owns the personal data and that the Data Subject retains ownership of their personal data.

GDPR provides updates to the EU's DPA, the Data Protection Act (1998), specifically the following:

- **Increased Territorial Scope** – GDPR applies to all organizations processing the personal data of EU residents, regardless of that organizations location, or where that data is hosted.
- **Breach Notification** - Breach notification to the supervisory body (the Information Commissioner's Office (ICO) in the UK), and the known affected Data Subjects, will be mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be issued within 72 hours of first having become aware of the breach. This includes notifying the Data Subjects.
- **Penalties** - A breach of the GDPR can incur significant fines, up to 4% of annual global turnover or €20 Million (whichever is greater).
- **Consent** - A request for consent to collect and retain personal data must be given in an intelligible and easily accessible form, by the Data Controller or Data Processor, to the Data Subject, with the purpose for data processing attached to that consent, using clear and plain language. It must be as easy to withdraw consent, as it is to give it.
- **Privacy by Design** - The Controllers will include data protection from the outset when designing new systems, rather than an optional extra.
- **Vendor Management** – It is the responsibility or organizations to comply with GDPR and they should provide evidence, either by assessment, or other means of clarification.

Data Subject Rights

Beyond seeking specific consent to use the Data Subjects personal information there are further rights extended to the Data Subject, by the Data Controller as follows:

- **Right to Access** – The Data Subject must be able to obtain from the Data Controller confirmation as to whether personal data concerning them is being processed, where, and for what purpose.
- **Right to Rectification** – When a Data Subjects data is found to be incorrect, or incomplete, the Data Subject can request that it is corrected.
- **Right to be Forgotten** - The right to be forgotten entitles the data subject to have the Data Controller erase his or her personal data, removing all instances.
- **Data Portability** - A data subject can request and receive the personal data concerning them in an easily readable format and have the right to transmit that data to another controller.
- **Right to Object** – The Data Subject has the right to remove consent to the processing of their data, at any time. Also included are Rights regarding restrictions of processing personal data, and the ability to request intervention, by a human, where machines undertake automated processing.

Governance

GDPR specifies the responsibilities of each organization maintaining a GDPR point of contact, the Data Protection Officer (DPO). The DPO is central to establishing and maintaining the core responsibilities of organization compliance. The regulation states that the DPO can be a member of staff or a trusted third party, not dictating that it be a full-time role, and only mandatory in certain circumstances (see below).

GDPR specifies mandatory requirement of a Data Protection Officer in the following instances:

- Public authorities.
- Organizations that perform large scale systemic monitoring of individuals.
- Organizations that perform large scale processing of special categories of data or data relating to criminal convictions and offences.

GDPR outlines the duties of the Data Protection Officer as follows:

- To inform and advise the organization and its employees about the obligation under GDPR (and other data protection laws that the organization may be subject to).
- To monitor compliance with the GDPR and other data protection laws, including;
- Managing internal data protection activities.
- Advising on data protection impact assessments.
- Training staff and conduct internal audits.
- To be the first point of contact for the supervisory authorities and for the individuals whose data is processed (employees, customers etc.).

FAQ's

Q. Does the normal confidentiality obligation between Doctor/Surgeon and their patient apply?

- Normal obligations do apply but you will need to obtain written consent from your patient. If you do not already have a signed agreement, then it would be best to have one in place.

Q. Can a patient request to change personal data when that is convenient for them?

- The *GDPR* includes a right for individuals to have inaccurate personal data *rectified* or completed if it is incomplete. An individual can make a request for *rectification* verbally or in writing. You have one calendar month to respond to a request. In certain circumstances you can refuse a request for *rectification*.

You can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, consider whether the request is repetitive in nature. If you consider that a request is manifestly unfounded or excessive you can:

- request a "reasonable fee" to deal with the request;

  You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual without undue delay and within one month. You do not need to comply with the request until you have received the fee.

- or refuse to deal with the request.
- In either case you will need to justify your decision.

Q. Can a patient ask to delete their patient record?

- It would be justifiable to retain information. Ideally this should be covered within the consent. GDPR does not override any prior or new "legal" obligation.

Q. If a patient is sexually active and has a high risk of STD's, can such a patient ask to remove that information?

- If they have agreed to the collection of their information, and it is relevant to the patient and that the risk of infection is real to the Doctor and/or third parties, the Doctor should keep the information, however, as you would expect it cannot be disclosed, shared or transmitted as it is classed as secret personal data.

Q. Do I need to appoint a Data Controller when my surgery consists of a Doctor and a member of support staff?

- The answer is no, you do not have to appoint a DC, however, you must appoint (identify) some person who is responsible for managing patients data.

Q. Due to the new GDPR regulations are we obliged to *destroy* all data after this retaining period or not?

- GDPR does not override any prior or new "legal" obligation. So you do not need to destroy patient information although and where possible, I would advise that you obtain written consent from your patients.

The overriding and clear message of this legislation is that In the first instance the data controller, (the doctor, office/practice manager) must provide assurance of data security. There are instances where a Doctor can overrule GDPR if there are legal or moral reasons pertinent to that country.

Please do not forget that if you are ever challenged, you must always obtain legal advice. It is always advisable to take independent legal advice as this document is merely a guide to the possible implications of GDPR.

To do's

Some steps you should take to protect yourself now.

- Make sure that your staff are aware of the implications of GDPR as well as how to handle data. You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.
- You should review how you seek, record and manage consent and whether you need to make any changes.
- Appoint a Data Controller. If you are a small surgery/practice this could be the person who manages your facility (Practice Manager) or the Doctor/Surgeon who runs the practice.
- If your facility handles information regarding patients travelling from another EU member state, you should determine your lead data protection supervisory authority.
- You should make sure you have the right procedures in place to detect and report a personal data breach.

Finally, the potential fines are hefty and could be ruinous for a small company or practice. It is therefore imperative to have proper processes, procedures, policies and insurances in place.