New General Data Protection Regulation; what does this mean for Dental Hygienists and Therapists?

The digital revolution of the past 20 years has made the level of data information sharing unprecedented and ubiquitous. We share with friends, family, and even strangers online. Companies share our data, often legitimately, sometimes circumnavigating laws to sell our personal information for a profit. To give greater control over personal data to individuals the European Parliament Council have drawn up a new set of regulations which supersede the previous EU Data Protection Directive (1995) and the UK's Data Protection Act (1998). The EU General Data Protection Regulation (GDPR) is due to come into force on 25th May 2018, and its aim is to protect individuals from privacy and data breaches in this increasingly data-driven world.

For most clinicians who are already adhering to existing data protection law in the way that patient information is recorded and stored, there may on the face of it seem little change. For those who own their own a practice the changes may be more apparent.

The key changes

- Increased territorial scope

The jurisdiction of the GDPR is greater than existing regulation. The applicability of these regulations is very clear – it applies to the processing of all personal data by controllers and processors based on in the EU, regardless of where processing takes place.

- Penalties for breaches and non-compliance

Organisations can be fined up to 4% of annual turnover for serious infringements e.g. not having sufficient consent to process data. A tiered approach to fines has been taken, for example a 2% fine can be imposed of smaller offences such as not having records in order (article 28). This applies to controllers and processors of data.

- Consent

The conditions for consent have been strengthened. Patient must of offered a genuine choice and control over their data is used. Consent must now involve clear affirmative action, for example the use of pre-ticked boxes is not permitted, nor is vague blanket consent to share and use personal data. It must also be as easy for a patient to withdraw their consent as it is for them to give it. Organisations can no longer use long illegible terms and conditions.

- Data Portability

This is a new introduction and given patients the rights to receive personal data concerning them and to pass that data to another controller i.e. practice.

- Right to Access

Patients have the right to obtain confirmation from the controller whether or not their personal data is being processed, where and for what purpose. This is a significant change to increase transparency for individuals.

- Right to be forgotten

Known as data erasure, this gives patients the right to have the data controller erase their personal data, cease further dissemination of the data (article 17). It should be noted that this requires controllers to compare the individual's right to the 'public interest in the availability of data' when considering requests.

- Breach Notification

Breach notification is mandatory under the GDPR where a breach is likely to 'result in a risk for the right and freedoms of individuals'. Notification of a breach must be made to the Information Commissioner's Office within 72hours.

- Data Protection Officers

Large companies (such as hospitals) are required to appoint a Data Protection Officer (DPO) if NHS patients are seen. This may also apply to some large or corporate dental practices. If the practice is private the appointment of DPO is not necessary, but it should be noted that this was considered and the reason for not appointing should be documented. The DPO should report to the highest level of management but not be in a position that can be coerced, nor should it be a member of management or owners.

- Privacy by Design

This concept has existed for some time but has now been formalised via the GDPR. 'Privacy by design' is the inclusion of data protection from the outset of designing information systems, rather than including this as an addition.

What does this mean?

There are two circumstances within the GDPR that permit the recording, storing and use of information about individuals; one of these applies to all information and the other is for 'special' information, which includes that related to health. Under this circumstance patient information can be used to meet contractual obligations i.e. providing dental care, complying with General Dental Council rules and standards, NHS regulations and tax laws. Information can also be used if patients consent has been obtained, but it is not necessary to rely on consent to keep and use patients' records in connection with the provision of dental treatment. For example, consent is not required to use patient information to send a routine recall email or text message, but if the same information was used without consent for marketing this would not be permitted. The Regulations are specific about when and how consent should be obtained and when a lawful alternative is more appropriate. In fact the GDPR states that consent is not inherently superior and can be difficult to obtain and manage with, '*consent is*

appropriate if a real choice can be made, but if not, asking for consent is misleading and inherently unfair' (Information Commissioner's Office, ND). There are six lawful bases for processing data under the GDPR listed in Article 6(1), and consent is one of them.

Increased transparency is one of the key principles of these Regulations. This means that all patients should be provided with detailed information about the information that is currently held about them and for what purpose. The GDPR calls this a 'privacy notice'. Another principle underpinning the Regulations is that of accountability. This means that clear and explicit procedures need to be in place with regard to patient confidentiality and how data is managed and stored. This is important to demonstrate how the law has been adhered to if the Information Commissioner's Office makes a compulsory assessment to check individual and practice compliance. To avoid accidentally or deliberately compromising patient data through unauthorised access care must be taken when using and storing data with particular attention being paid of online security measures. All changes to patient's individual data should be logged in their notes, showing a clear audit trail. If overall changes are made to data management or storage in a practice this will need to be logged and updated in policies and procedures, as well as telling all patients how and why this has happened i.e. a privacy notice needs to be sent. If it is necessary to seek help with computer systems that hold patients records from an IT expert, it is important to check that that they also understand and adhere to the GDPR. This should also be reflected in their contract.

Much of the work currently carried out by Hygienists and Therapists complies with the GDPR. It will be when starting work at a new practice, or setting up a practice, that consideration will need to be given to how information is obtained, how and when it can be used, who has access to it, and how it is stored. When Britain leaves the EU in 2019, it's likely that these regulations will remain as part of the transition arrangements. Therefore knowledge of your duties in this regard may also become part of compulsory continued professional development requirements.

For more information see 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now' published by the Information Commissioner's Office.

References

European Union. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* Available at: http://eur/lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (Accessed 2April 2018)

EUGDPR.org. *The European Union General Data Protection Regulation is the most important change in data privacy regulation in 20 years – we're here to make sure that you are prepared.* Available at: https://www.eugdpr.org/ (Accessed 2 April 2018)

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Accessed 2 April 2018)

Great Britain. Data Protection Act 1998: Elizabeth II. (1998) London: The Stationery Office.

Information Commissioner's Office. *Guide to the General Data Protection Regulation (GDPR)*. Available at:https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (Accessed: 2 April 2018).

Information Commissioner's Office. *Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now.* Available at: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf (Accessed: 2 April 2018)