HOW DOES THE NEW GDPR AFFECT MY PRACTICE?

Dr Martin Foster, Head of Dental Services for Ireland, explains how the new General Data Protection Regulations (GDPR) impact your everyday work

Friday 25 May 2018 is 'GDPR' day – from this date the new EU regulations on data protection become the law in all member states and replace the previous legislation. The new law has been set out to take account of the fact that life now involves much more 'digital' activity than before and is a challenging environment for protecting personal information. The new law sets out to address this challenge.

WHAT DOES IT MEAN FOR MY PRACTICE?

All data controllers and data processors are affected, therefore all dental practices need to comply with the new law. This involves also being able to demonstrate compliance. Failure to do so can result in serious penalties being imposed.

The Data Protection Commissioner (DPC) has issued guidance on the new requirements and this is available from **dataprotection.ie**.

DATA PROCESSING

The processing of data includes collecting, storing, using, disclosing (and destroying) personal information such as dental records. The GDPR requires that:

1. there must be a "legal basis" (a valid reason) for holding personal information
2. this legal basis is made clear to patients.

In dental practice, the relevant "legal basis" is likely to be that the data processing is necessary for the provision of treatment by a registered dental professional.

Another basis is the consent of the patient to the processing of their data.

As with any consent process of course, it is essential that the patient's agreement is based upon an accurate understanding of the reason for the processing, the patient has the freedom to choose and withdraw consent, and the information is used only for the purposes for which it was given. For example, a patient must have given specific consent to receive communications from the practice by phone or text.

The GDPR requires that compliance can be demonstrated, so it is essential that there is clear documentary evidence that the patient has given consent for their information to be used.

TRANSPARENCY AND FAIR PROCESSING

The regulations require that a dental practice must inform patients about what is done with their personal information. To comply with this, patients should be provided with a "privacy notice" when information is collected. A notice should advise the patient:

- who the data controller is (for example, who is responsible for safeguarding their information) and the relevant contact details
- the purpose for which the information is required
- the legal basis for processing the information
- the categories of personal data concerned
- who might have access to the information
- how the information is protected
- the rights of the patient including advice that the patient can complain to the DPC if there is any concern about how their personal information is being managed.

PATIENT RIGHTS

The GDPR gives patients more rights with respect to their personal data.

As with the previous legislation, a patient will have the right to be provided with copies of the information held, however the period a practice has to comply with such a request is reduced to one month. Information must be provided without charge unless the request is unreasonable or excessive. If the decision is made to refuse the request, the reason for this must be provided and the patient informed that they can raise the matter with the DPC.

Patients have greater rights in respect of rectifying and erasing records, and

READ THIS ARTICLE TO :

- Find out how the new regulations affect you at work
- Discover practical steps to help you comply with the new law

also with objecting to and restricting processing. There is a right of data "portability"– patients should be able to move their data from one data controller to another more easily and receive information in a structured, commonly used format. It is important that practices have systems that can cope with these requirements.

DATA BREACH

Should there be a breach of patient confidentiality, the data controller must notify the DPC without delay and, if possible, within 72 hours of becoming aware.

The patient must also be informed if the breach has a high risk of affecting their privacy rights. The new regulations provide for higher penalties for data breaches.

DATA PROTECTION IMPACT ASSESSMENT

Such assessments are a means of demonstrating measures in place to safeguard patient information. These assessments are legally required if the way in which information is handled has the potential to breach confidentiality. For example, the installation of new patient record software or a new system for sharing information or making referrals.

DATA PROTECTION OFFICER

There is a requirement that a Data Protection Officer (DPO) should be appointed within any organisation involved in processing patient information on a "large scale".

What constitutes "large scale" is not defined but based upon the guidance at present it would appear that hospitals, large multi-clinics or chains of practices would require a DPO whereas an individual practitioner would not. Where the line is drawn however is not specified, but the number of individuals for whom information is held will clearly be a major factor.

If there is any doubt about the requirement for a DPO, until further clarification is available, it would be advisable to carry out a self-assessment of your own practice in terms of the amount of personal data processed, both in terms of patient and staff records. Once this is done, the conclusion of the assessment should be documented including the decision on whether or not a DPO was considered necessary. In this way, it will be able to demonstrate that steps were taken to ensure compliance with the regulations.

If it is considered appropriate to appoint a DPO, the next step is to ensure that the relevant individual can carry out this role which involves monitoring and advising on the practice's compliance with data protection requirements.

The role should not be discharged by the same person who is responsible for decisions on and implementing data protection measures in the practice.

The DPC has helpful guidance relevant to the appointment of a DPO at dataprotection.ie

PRACTICAL STEPS

1. Document -
   a. the nature of all personal data held
   b. how it is collected
   c. how it is stored
   d. who has access
   e. who it is shared with
2. Ensure there is a legal basis for processing data. If based upon consent there must be an appropriate system in place for recording this.
3. Ensure "privacy notices" comply with the GDPR.
4. Decide if a DPO is required. If so ensure he/she has appropriate knowledge.
5. Have process for providing copies of patient records in an appropriate format promptly.
6. Have a clear procedure for reporting data breaches to the DPC.
7. Make sure that all staff are aware of the need to comply with the GDPR.

Ensure that you keep up-to-date with the information available at **dataprotection.ie** and **gdprandyou.ie**.

IN SUMMARY

The take home message is that practices need to be completely open and transparent about why personal data is collected and what it is used for. It is also necessary to be able to clearly demonstrate how data is safeguarded and processed.

MORE SUPPORT

Dental Protection is keen to encourage members with efforts to meet the requirements of the regulations. Our team of advisers are happy to assist with any queries you may have in relation to the new law. Please call **+44 113 241 0200** or email **enquiries@dentalprotection.org**