HOW TO BE READY FOR GDPR!

On 25th May 2018, the way in which we handle data will undergo a substantial change. The Data Protection Act will be supplemented by a new set of regulations known as the General Data Protection Regulation ("GDPR").

The concepts in the GDPR will not replace those already contained in the DPA but will add to the protections which the DPA provides. Therefore, if your dental practice already complies with the current law, this can serve as the starting point from which to ensure GDPR compliance.

GDPR however is new and there will be responsibilities upon you that have not been present before. The General Dental Council, is at the time of this article, not proposing to offer specialist training on GDPR and seems to be leaving it to practitioners themselves to ensure compliance.

In a large practice this could have significant implications. The GDPR places greater emphasis on the documentation that you as the data controller must keep to demonstrate accountability.

Compliance will require practices to review their approach to governance and how data protection is handled.

1. Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one. Implementing the GDPR could have significant resource implications, especially for larger organisations. You may find compliance difficult if you leave your preparations until the last minute.

2. Information you hold

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 across the organisation. The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own

Jonathan Jacobs
Head of Healthcare
jjacobs@anlaw.co.uk
T: - 01925 634681

records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3. Communicating privacy information

You should review your current privacy policy and put a plan in place for making any necessary changes in time for GDPR implementation. When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

4. Patients' rights

You should check your procedures to ensure they cover all the rights your patients have, including how you would delete personal data or provide data electronically and in a commonly used format. The GDPR includes the following rights: -

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- the right not to be subject to automated decision-making including profiling.

The right to data portability is new. It only applies to personal data an individual has provided to a controller where the processing is based on the individual's

Jonathan Jacobs
Head of Healthcare
jjacobs@anlaw.co.uk
T: - 01925 634681

consent or for the performance of a contract and when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide the information free of charge.

5. Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

6. Lawful basis for processing personal data

Many practices will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that patients will have a stronger right to have their data deleted where you use consent as your lawful basis for processing. You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements.

Jonathan Jacobs
Head of Healthcare
jjacobs@anlaw.co.uk
T: - 01925 634681

7. Consent

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data. You are not required to automatically refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

8. Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity. For the first time, the GDPR will bring in special protection for children's personal data, The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

9. Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. The GDPR introduces a duty on all practices to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases. You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would

Jonathan Jacobs
Head of Healthcare
jjacobs@anlaw.co.uk
T: - 01925 634681

be required to notify the ICO or affected individuals if a breach occurred. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself. You will also be required to inform the CQC of any data breach and it will be a matter for them and the ICO to determine the severity of the breach and what is th06+e appropriate action to take.

10. Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your practice's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer (DPO).

Jonathan Jacobs
Head of Healthcare
jjacobs@anlaw.co.uk
T: - 01925 634681