Nigel Knott
DOI: 10.1308/rcsfdj.2018.1

The General Data Protection Regulation

by Nigel Knott

What the GDPR will mean for the profession as it faces the biggest technical shake-up...

Author: Nigel Knott, Dental Surgeon and CEO of Dentsure Ltd, 6 Union Road, Chippenham, Wiltshire SN15 1HW
E: njk@dentsure.co.uk

Keywords: GDPR, Compliance, Analog, Digital, Security

Nearly 20 years have passed since data protection became enshrined in statute law and a failure to comply became a criminal offence. At the 2016 Annual Data Protection Practitioners' Conference, the headline topic addressed by the Information Commissioner was '*20 million reasons for organisations to get EU data reforms right*'.[1] His opening address included reference to $20 million (£17+ million) being the new maximum financial penalty for breaches of the General Data Protection Regulation (GDPR) that comes into effect on 25 May 2018.[2]

The principal reason behind this massive increase from £500,000 is to deter those who continue to ride roughshod over the requirements of the Data Protection Act 1998 (DPA). However, it seems to me that many of the techie thoroughbreds (Google, Facebook, YouTube, Twitter) have already bolted, with huge amounts of personal data being carried into the commercial marketplace and converted into cash. The anarchic activities of these tech giants have been largely responsible for the introduction of this latest piece of legislation. Although the lawyers will be rubbing their hands with glee, dentists will be wringing theirs at the prospect of dealing with yet more suffocating regulation, proscriptive bureaucracy and administrative expense. That is not to say that the GDPR is unnecessary but it adds to an already complex layer of professional regulation that requires an understanding of information and communications technology (ICT).

Senior staff at the General Dental Council (GDC) and Care Quality Commission (CQC) offices will no doubt be burning the midnight oil as they pore over the latest legislation, and the cost of insurance premiums for dental protection will presumably rise once again. I have located a law firm in Surrey, which sells technology and internet contracts, advertising an editable DPA privacy policy template that runs to 18 pages of A4, including 7 pages of instructions on how to modify it for a variety of different situations!

The implications of the GDPR in dental practice

In many respects, the GDPR is designed to reinforce the DPA regulations but it also adds new aspects of data protection resulting from the explosion in cybercrime and the commercial exploitation of sensitive personal data for illicit purposes. It is evident from dental practice websites that the profession has been notably slow in implementing DPA compliance measures. The patient data that registered dentists process are now classed as special category data, with higher levels of regulation and scrutiny being imposed on processing this type of data. The government has published a new Digital Charter,[3] and the Department of Health and Social Care has updated its requirements concerning data security and protection in the National Health Service.[4] These should be added to the list of essential documents for bedtime reading between now and the end of May!

The introduction of the GDPR requires the appointment of a data protection officer (DPO) in every dental practice, whose job it will be to record and control all online and offline data created/stored/processed/transferred/shared both within and outside the dental practice premises. The DPO must maintain a tight control over all data-processing activity involving in-house dental practice computers, the practice databank, offsite online/offline e-data storage and mobile devices (mobile phones, laptops, flash drives, memory sticks etc), as well as internet activity.

Some formal knowledge in computer studies will assist in understanding the risks involved and the need to introduce a documented data protection privacy policy.[6] The DPO will carry the can for future breaches of the law and every member of the dental practice team needs to understand their own responsibilities whenever they process, store, share or transfer sensitive patient data. The role of dental associates in their DPA duties and responsibilities concerning the practice patients needs to be legally binding.

Gone are the days when the practice owner could lock up the surgery premises, safe in the knowledge that the patient records were secured in a metal cabinet with only fire and flood to worry about. The advent of computers and use of the internet has changed all that, and what might be considered the halcyon days of dental practice are now dim and distant memories of the past.

The application of computer technology and the digitisation of dental surfaces have transformed the dental world. The recent introduction of 3D printing techniques used to laser sinter titanium powder into a precision-fitting dental prosthesis is truly incredible. This process depends on the creation of massive amounts of digitised data, all of which have to be carefully processed and safely stored. The electronic networks used to transfer these large data files (known as STL files) to remote manufacturing facilities need to be safely secured with no possible risk of patient data being intercepted or corrupted.

A serious weakness at the heart of the dramatic changes in technology powered by computers (CADCAM) is the lack of formal education and training in their function and use at undergraduate and postgraduate levels. Dental prosthetics used to include the practical training of dentists in the laboratory and formed part of an integrated undergraduate curriculum. Many dentists were well capable of carrying out their own prosthetic work in a dental laboratory facility in the dental practice itself. Casting precious and non-precious metals, sintering porcelain powders and setting up/articulating artificial teeth was not uncommon – but now the scene has changed dramatically.

Too few dentists today have sufficient understanding of what is actually going on in the dental world of digitised technology to recognise and quantify the risks. We are faced with having to provide our patients with the same high standards of cyber service that they customarily expect to receive from us in the real offline (analog) world. There must be no unpleasant surprises hidden

away in the artificial/virtual arena, where the same offline principles must be applied. Our patient profiles nowadays comprise all age groups and we have to cater for older-generation technophobes as well as young technophiles. This is a most complex and difficult period of transition for all those who work in dentistry, and we must ensure we deliver exactly what is written on the tin!

The offline (analog)/online (digital) interface

Some simple comparisons may prove helpful in understanding the difficulties we face in dental practice while we metamorphose from the traditional offline (analog) to the online high tech (digital) environment. In some respects, we are encountering the problems the profession faced many years ago when x-rays were first introduced. X-rays were known to have dangerous implications but nobody at the time could have foreseen the extent of the damage that later became so obvious, with such malignant effects. Our knowledge and experience of creating radiographs, computed tomography scans, etc, has enabled us to develop effective preventive measures, and so it must be with patient e-data protection and the use of the internet.

In the analog world, the hacking of telephone conversations is a well-established crime and the Royal Mail service is similarly protected from unlawful intrusion. Items of particular importance can be delivered to you with an added layer of security purchased with tracked guaranteed delivery status. The traditional analog sealed letter carrying a postage stamp and delivered by hand to your practice address, however, is fast being replaced by the electronic mail (digital) equivalent that (like an x-ray) may be accompanied by unpredictable risk. The free email services are like unstamped postcards that can be read by anybody and have no security or privacy status whatsoever.

We are encountering the problems the profession faced many years ago when x-rays were first introduced.

Indeed, this clever invention has delivered huge wealth to the big techies (internet service providers [ISPs]) financing these services in return for their being able to access the information and sensitive personal data freely given by the sender and use it for commercial purposes. Do you ever read the small print of the conditions of use accompanying these free services before you agree to their terms?

Although there is never a free lunch, it amazes me how few users of email and the internet truly understand the implications of free usage and the risks involved. Now the GDPR has arrived, you will need to do so – and fast! I am not suggesting we behave like technophobes and practise the rituals of the druids, with written/cyber records being forbidden, but the introduction of a sensible blending of processes designed to deliver safely the enormous benefits of both digital and analog routines.

The principles of good data protection

In a nutshell, patients need to be reassured that the conditions for processing their sensitive personal data are solely for the purpose of maintaining their wellbeing and that the dental practice will use this data in their best interests at all times. Patients must be reassured that having entrusted us with sensitive personal data, it will be used responsibly in their legitimate interests. All healthcare professionals must understand that patient confidentiality is a precious part of the trust that patients place in us. Only the minimum amount of data absolutely necessary to provide patient services should be processed, and all data must be accurate and stored no longer than is required by law in a secure environment.

Special attention should be paid to the security of any data being transferred/shared with third parties either offline or online and patient consent must be obtained for their preferred method of safe communication with their dental practice. A choice of secure communications must be documented and telephone, letters sent by post or secure email should be offered as a preference to every patient. Text messaging should not include unsecured sensitive patient data. It is not permissible to state that 'the practice complies with all aspects of the DPA' in the absence of the DPO documenting and publishing a detailed practice privacy notice in the practice waiting room and on the practice website. Default electronic opt-in choices are unacceptable.

Dental practice websites

Websites are classified as 'information-only' or 'interactive/transactional', where templates exist for the harvesting of patient data and there are hyperlinks to other websites. Of particular concern with interactive website facilities is the provision of contact us/referral/feedback/complaints templates with no special security measures in place to encrypt sensitive patient data while being transferred from the website to the dental practice (or elsewhere) for processing. New GDPR legislation requires a 'just in time' notice to inform all website visitors of the security status of any data harvesting/data transfer facility.

There can be no excuse for continuing to use or advertise insecure email services for professional purposes, as this is an area where DPA compliance is now an imperative. It is noticeable in the latest wave of regulation that ISO 27001 is specifically mentioned as the necessary information security standard of compliance that you must use at all times where your online activities are concerned. The status of any practice email hyperlink on your website must be security classified.

All dental practice principals are advised to review their website architecture and content, with written contracts being in place with software suppliers and ISPs. It is particularly important to include details of your registration with the ICO, the name and contact details of the DPO, and a privacy notice. Interactive transactional websites should have transport layer security protection, with padlocked (https://) access informing your patients, that they are visiting a trusted-access website.

The professional use of email

Perhaps the greatest unseen threat to the integrity of sensitive patient data is the casual use of insecure email services by members of the dental practice team. Untutored staff will always be the weakest link, and a quick trawl of practice websites reveals far too many insecure email contact addresses (and URLs [uniform resource locators]) that fail to comply with DPA, GDC and CQC regulations.

The CQC has to ensure the safe handling and storage of all patient records. I have little doubt that from 25 May 2018, their practice investigations will include website compliance, communications and email service status. This will be an easy armchair task for compliance officers as the clues will be there for all to see on a screen. Some websites ooze class and an online peep inside practice premises serviced by a highly qualified practice team gives online visitors a taste of what is on offer. These are the high street shop windows of dentistry and Google or Firefox will soon reveal the secrets inside.

The new GDPR rules will bring much-needed change, and the profession must become accustomed to having to resource safe and secure professional email services and secure website-hosting facilities. My advice is to find a company that ticks all of the security/customer care boxes (including round-the-clock telephone IT support) and has ISO 27001/9001 accreditation. A suitable service provider will be familiar with contractual documentation concerning the services they offer. Some specialist service providers are including GDPA seminars/webinars as part of their menu. Again, I think it is important that your DPO and preferably all the staff from your practice attend as part of their continuing professional development. In future, 'medical in confidence' items will need to be treated accordingly with an additional layer of encrypted protection that will be available with ISO 27001 certificated services.

Conclusions

Although the GDPR is unlikely to impose unpleasant physical damage reminiscent of the early days of x-rays, it will bring some difficult and maybe expensive decisions to the fore. The Spectre and Meltdown security vulnerabilities and computer viruses such as Melissa, MyDoom and Stuxnet should be enough to frighten most practice principals into carrying out a comprehensive study of their practice ICT systems. I feel sure the specialist dental software suppliers will welcome an industry-wide GDPR compliance initiative to preserve the necessary confidence and trust in a risk-conscious profession. The ICO website provides comprehensive advice (digital), excellent online guidance notes and a helpful telephone service (analog).

May Day will have a new dimension this year for dentists, who will need to have completed a comprehensive review of the DPA/GDPR and implemented the requirements. For good measure, they should sign up for the free online ICO monthly newsletters[7] to keep in touch with news on data protection.

GDPR checklist

- Appoint a DPO.
- Ensure your practice is correctly registered/notified with the ICO.[8]
- Document and publish a practice privacy notice.[6]
- Pay particular attention to your online/offline communication security.
- Maintain written contracts with ISPs.
- Ensure your professional e-communications (email) are DPA compliant.
- Check your practice website is DPA-compliant.
- Record and report breaches of Privacy and Electronic Communications Regulations 2003.[9]
- Practice principals should review all employee/self-employed (associate) contracts to include security restrictions on patient data processing.

References

1. Information Commissioner's Office. *'20 million reasons for organisations to get EU data reforms right'*. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/03/20-million-reasons-for-organisations-to-get-eu-data-reforms-right/ (cited February 2018).
2. Information Commissioner's Office. *Guide to the General Data Protection Regulation (GDPR)*. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ (cited February 2018).
3. GOV.UK. *Digital Charter*. https://www.gov.uk/government/publications/digital-charter/ (cited February 2018).
4. Department of Health and Social Care. *2017/18 Data Security and Protection Requirements*. London: DHSC; 2018.
5. Information Commissioner's Office. *Documentation*. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ (cited February 2018).
6. Information Commissioner's Office. *Privacy notices, transparency and control*. https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/ (cited February 2018).
7. Information Commissioner's Office. *E-newsletter*. https://ico.org.uk/about-the-ico/news-and-events/e-newsletter/ (cited February 2018).
8. Information Commissioner's Office. *Register (notify) under the Data Protection Act*. https://ico.org.uk/for-organisations/register/ (cited February 2018).
9. Information Commissioner's Office. *Notification of PECR Security Breaches*. Wilmslow, UK: ICO; 2013.