DENTAL FOCUS

GDPR - WTF?

A guide to cutting through the noise and getting the right things done.

WRITTEN BY MADDY WHITFORD

Dental Focus specialise in creating compliant websites, giving dentists peace of mind with GDC, CQC and ICO compliance because our family background in dentistry is at the heart of everything we do. Maddy Whitford is Business Manager at Dental Focus and has a growing passion for improving company systems to ensure clients are attracting patients with their Websites, Google SEO and Social Media.

Do you know who has your personal data?

The world has changed, and we are accustomed to sharing our data in so many different ways on a daily basis without even thinking about it. Every single day we are giving our personal data away with no clue about what it will be used for, who it will be shared with, where it will be stored, or when it will be kept until.

Think of your hotel reservations, your gym membership, restaurant bookings. Think about the free wifi services that you use at coffee shops and in pubs or restaurants, and the websites that you browse which have the 'cookie policy' notice. What about every time you fill an enquiry form or make a phone call and hear that 'this call is being recorded'?

Do you know what your rights are in regards to the data that you share?

The GDPR will become the law on the 25th May 2018. The regulations address how organisations collect and store personal data, which is defined as any data which could be directly or indirectly identifiable, and the rights of the individual to have control over this data and how it is used. What you have to do and take into account to protect your patients' data, others have to do to protect your data too. We are doing this for each other.

The Information Commissioner's Office (ICO) have shared guidance on how to comply with upcoming GDPR enforcement, which replaces the existing Data Protection Act 1988 (DPA) laws, but even so a cloud of uncertainty around this imminent change has been apparent for months, and may be stopping many from taking the necessary action to protect themselves and their patients.

Health-related data is listed by the GDPR as a 'Special Category Data', meaning that it has been flagged up as more sensitive and needing more protection than other areas. Dental practices are therefore likely to be among those that come under more scrutiny in terms of how compliant they are with the regulations.

The maximum fine of £500,000 for data protection breaches will be raised to a shocking €20,000,000 (or 4% of your business revenue, whichever is greater!), and although the UK Information Commissioner has publicly said 'issuing fines has always been and will continue to be, a last resort'[1], the huge increase in the maximum fine should be an indicator of the fact that they are taking data protection very seriously.

It is crucial that you and your team are aware of what GDPR is, what needs to change, and what needs to be done on an ongoing basis to stay

1 https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/

compliant. Your whole practice should be able to help identify current areas of your operations that could be affected by GDPR.

ACTION POINT:

There should be one assigned Data Protection Officer (DPO) who has the accountability, knowledge, support, and authority within the team to fulfil their duties in vigilantly ensuring that practice systems and processes are compliant. Consider whether you wish to appoint yourself, someone within your team, or an external Data Protection Advisor for this role because although it may be tempting to add it to a team member's existing responsibilities, you need to be confident that it is being treated as a priority and given the time and attention that is needed.

Knowing What You Know

A solid awareness of the different types of data that you collect and how you collect it is the first step to cutting through the noise. Once you have systems in place to log this information, you can analyse and log how each type of data is stored, used, and shared which will give you a much clearer understanding of what you need to do to fulfil your responsibilities and remain compliant.

This means that initially, you will need to do a full analysis of the different ways in which you collect personal data - that is, receive and store any information about individuals. Once you've examined and listed the various **ways** that data is collected, you should consider for each one:

- **Where** is the data stored
- **What** do you use it for
- **Who** do you share it with
- **When** do you keep it until

Remember that you collect data in a myriad of ways - new patient registrations, website form enquiries, phone call recordings, website cookies, facebook messages, before and after photos, video testimonials and many others. There are many areas to consider outside of the standard patient management system.

ACTION POINT:

We recommend creating a shared logbook which details this information, because in the future, if an individual exercises one of their rights (for instance, the right to erasure, also known as 'the right to be forgotten'), this reference sheet will allow you to quickly identify each of the locations in which data may be stored about them which in turn will allow you to fully honour the request.

Your Privacy Policy

Measures should be taken to ensure that when new personal data is being collected, you always receive the appropriate consent and the individual is fully informed about how you intend to use their information, what your lawful basis for processing their data is, your data retention periods, and that they have the right to complain to the ICO if they feel that there are any issues with how you handle their data. This information is usually provided in the form of a Privacy Policy which should be linked to on your website as well as being physically available within the practice.

ACTION POINT:

It's time to review your Privacy Policy and ensure that you have included:

- A lawful basis for processing data (the majority of the time this will be consent, explained in further detail below)
- Your data retention period (how long you intend to store the data - 'indefinitely' is the simplest option to reduce admin work)
- The rights of the individual, which are explained in more depth towards the end of this article:
  - 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
  - Rights in relation to automated decision making and profiling.
- Who at the practice an individual should speak to to exercise any of these rights.
- The notice that an individual has the right to complain to the ICO if they think there is a problem with the way you are handling their data.

Your Privacy Policy should also outline if you intend to share the collected data with any third parties, and it should include links to each third party's own Privacy Policy as well as to your Cookie Policy. Consider if you need to include links to the Privacy Policies of both Google and Facebook, because many websites do have tracking scripts and cookies for both of these giants to collect data about the visitors to your website. Ensure that you are happy with the Privacy Policy and standards for data protection of any third party that you choose to share data with.

Explicit Consent

To use consent as your lawful basis for processing data, you must make sure that you alway receive explicit consent when individuals share any personal data with you.

In the past, it has been sufficient to have pre-ticked opt in boxes or to assume consent as a result of inaction (as you will have seen with the Cookie Policy notices that pop up when you visit websites - unless you take action, they assume that you agree to accept cookies). Now, consent cannot be implied and must be specifically given by an action of the individual.

Consent should also be specific, and therefore it is necessary to request separate consent for the collection and storage of patient data, and the subsequent use of that data to market to the individual. Website forms should have two 'opt-in' tickboxes:

- Required Opt-in field (form will not be submitted without this ticked) to consent to collecting and storing personal data for the purpose of communications and providing a service.
- Optional Opt-in field to consent to collecting and storing personal data for the purpose of communications and marketing.

If your website forms currently link to any Customer Relationship Management (CRM) systems which automatically sign an individual up to receive a marketing newsletter or newsletter sequence, you need to ensure that if they have not ticked the 'Opt-in for communications and marketing' box, they do not get added to this mailing list or receive any newsletter or sequence.

The same checkboxes should be added on all of your paper forms, with the whole team aware that the 'Required Opt-in field' must alway be ticked by the patient before forms are accepted.

Requests for consent should always be accompanied by a copy of or link to the latest up-to-date Privacy Policy.

ACTION POINT:

Consider each of the ways in which you collect data from the list that you have already created, and make sure that for each of them you are getting explicit consent to a) collect and store the data and to b) communicate for marketing.

What about your existing data?

You already have a patient database full of personal information and you already communicate with patients regularly.

Luckily, you are not required to regain consent for all of this patient data for you to continue to communicate with them to do anything that is necessary to fulfill the role that they would expect of you as your patient, such as sending appointment confirmations or reminders. What you should do is email everyone your new and updated Privacy Policy.

ACTION POINT:

You do however need to regain consent to market to this database, unless you were already collecting explicit consent for marketing when collecting data. Anyone who has not opted in and consented to marketing communications will need to be removed from marketing mailing lists and should receive no further marketing communications. When you email out the Privacy Policy, you can also ask them to opt-in to marketing.

Individuals' Rights

It's important to be aware of what rights individuals have because in most cases if they make a request you will be expected to respond within one month, a slight reduction from the previous 40 day time to respond. In the majority of cases, if the individual is within their rights, you cannot charge for honouring this request.

The earlier-mentioned 'logbook' is invaluable in this situation, because you will need to have the ability to quickly locate all of the information that you hold on one individual and take the necessary action.

The right to be informed

This is about informing individuals **before** you collect their data that you are going to do it, how long you plan to store it for, and who you will be sharing it with. This is addressed by the mandatory consent with reference to an updated Privacy Policy.

The right of access

Individuals may request that you provide them with the personal data that you hold about them.

The right to rectification

This gives individuals the right to have inaccurate or incomplete personal data corrected. If you have already shared the data with any third parties, you must also contact them so that they can correct their own records.

The right to erasure

This is also known as 'the right to be forgotten'. Individuals may request that personal data about them is erased. Again, if you have already shared the data with a third party, you must also contact the third party so that they can also erase the data from their records.

The right to restrict processing

Restriction of processing means that you can store the personal data that you have collected but you cannot use it.

The right to data portability

The right to data portability allows individuals to get their personal data to use for their own purposes across other services. If they make this request, you

must provide them their data in a commonly used and machine readable form - for instance, a CSV file.

The right to object

Individuals must be informed of their right to object, which will be covered in your updated Privacy Policy. As soon as you receive an objection, you must stop using personal data for direct marketing processes.

The right not to be subject to automated decision-making including profiling

Automated decision-making can only be carried out with the individual's explicit consent - for example, if on a website form, they choose 'Invisalign' on a dropdown form asking which treatment they would like more information about, then you could enter them into an Invisalign marketing campaign. However, without this option being specified, you could not make the assumption that they are interested in Invisalign and enter them in a specific targeted Invisalign marketing campaign that is not being run for all other individuals.

The Best Practice

Remember that you have a responsibility to protect personal data that is shared with you, and to ensure that there are no breaches of that data. The data should only be used for the purposes outlined in your Privacy Policy and should only be shared with third parties that you trust to treat the data responsibly and with care.

Website and email security must be considered because if there is a data breach as a result of inadequate security measures, this will be your responsibility. When so much data is shared over email and through websites, it is of paramount importance that the protection of this data is treated as a priority.

SSL Encryption on the website encrypts the end to end transmission between the browser and the server, which means that when someone is browsing your website or submitting details via your website form, the information that they are looking at or submitting is not plain text and easily readable by eavesdroppers. For example, if somebody is using wifi in a public place, usually this is not secure and anyone with eavesdropping software could see what is being transmitted. SSL Encryption prevents this. SSL Encryption also helps to create a feeling of trust in a world of mistrust because in the address bar, the 'Not Secure' message is replaced by a 'Secure' message and padlock.

Email is not generally encrypted and therefore should never be used to send personal data or patient information outside of the practice - this includes to clients or to other professionals. The best practice is to use email to notify patients to call the practice, but never to transmit any personal information, just like your banks do. However, email can be used securely within the practice if the correct precautions have been taken. Solutions such as Microsoft Office Exchange 365 email accounts

ensure that internal emails are encrypted both at transmission and at rest. That means that if you are using Microsoft Office 365 (O365) and the recipient is on the same O365 network as you, your emails are encrypted during transmission.

The Horse's Mouth

There is a whole host of information available about GDPR. The ICO have published a Guide to the GDPR that should prove a comprehensive reference point should you wish to find out further information:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

About the Author

Maddy Whitford is Business Manager at Dental Focus and has a growing passion for improving company systems to ensure clients are attracting patients with their Websites, Google SEO and Social Media. Dental Focus specialise in creating compliant websites, giving dentists peace of mind with GDC, CQC and ICO compliance because our family background in dentistry is at the heart of everything we do. More information at www.dentalfocus.com.