Sandes Avenue Dental Practice

Information Commissioner's Office

G.D.P.R

"The general data protection regulation (GDPR) is a new EU law that will come into effect on 25 May 2018 to replace the current Data Protection Act. It's the biggest overhaul of data protection legislation for over 25 years, and will introduce new requirements for how organisations process personal data. And before you wonder what will happen after Brexit, it's been made clear that all businesses and charities will have to comply, which means it is likely we will adopt all or most of GDPR as domestic legislation." (The Guardian 5th May 2017)

1) Awareness

The first part of the implementation of the new GDPR regulations is to make the key people (the team and patients) aware of what the changes are and how we are implementing them. We are already constantly ensuring we are compliant with Data Protection but the GDPR supersedes DPA by not only ensuring we are transparent about who we are and how we intend to use collected information, but to now explain our lawful basis for processing the data we collect, our data retention periods and the pathway for an individual to complain to the ICO if they feel we are mishandling their information.

The GDPR also enforces that the information which is to be provided must be clear and concise and easy to understand; so avoid jargon and abbreviations (unless universal) and factual. The Principal Dentist; Dr. Iqbal, is the Data Controller for the practice. This means he has full control over all the records; how they are stored, accessed and deleted. The associates and therapists/hygienists are classed as Data Processors and need to be registered with the ICO and have a Data Processer contract. The laboratories, other service providers (where we refer) computer software provider, the computer support company, the membership plan provider and the accountants will all have a Data Processor contract with us. The employees work under the Data Controller's instruction so will not be classed as Data Processors.

Some points to remember:

- Individuals have the right to be informed about the collection and use of their personal data. *This is a key transparency requirement under the GDPR.*
- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- It is often most effective to provide privacy information to people using a combination of different techniques including layering, dashboards, and just-in-time notices.
- User testing is a good way to get feedback on how effective the delivery of your privacy information is.
- You must regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual's personal data to their attention before you start the processing.
- Getting the right to be informed correct can help you to comply with other aspects of the GDPR and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

2) Information We Hold

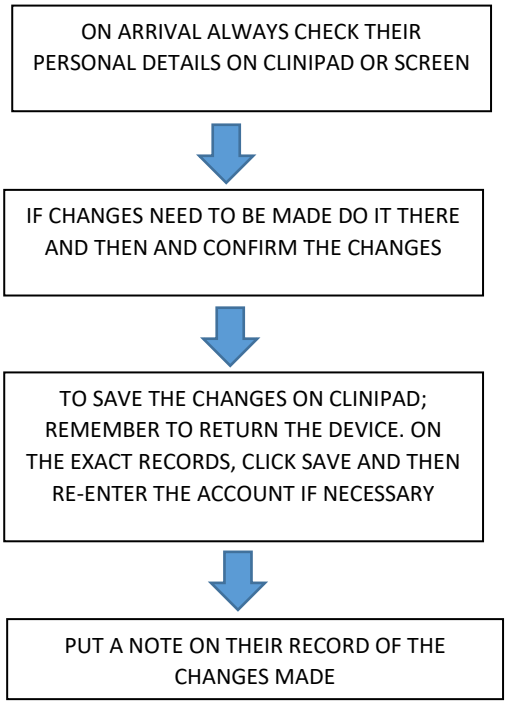
How do we document the information we hold and ensure it is up-to-date, that we know where it came from and who we share it with?

We have introduced maintenance records of the information we hold; initially an information audit and further records include: 'information changes and updates', 'record of archiving', 'record of destruction'. Below is the process of how we will audit and update, or destroy records:

Patient information (regular/current patients):

a) Check for any changes on every visit
b) Amend any information on patient's record to reflect current dentist etc.
c) Ensure any changes are recorded immediately and accurately
d) 'Paper Trail' the changes
e) Record who we share patient information with**

This process has been mapped out to ensure full understanding of how our duties have changed:



Patient information (leaver):

a) Do an Information Audit (paper and computer)
b) Check how long patient has not attended for (check policy for more detail). **This process has been mapped out to ensure full understanding of how our duties have changed:**

< 11 years paper: scan onto Exact and put a note to say when scanned and when and how the paper record was destroyed and archive (but do not delete the computer record)

< 11 years computer: leave on Exact and put a note on to say when checked and archived but do not delete

> 11 years paper: Where no computer record exists destroy the paper record and fill out the record archive of patient name & d.o.b. If there is a computer record also, put a note to say when and how the paper record was destroyed and archive (but do not delete the computer record) and fill out the record archive of patient name & d.o.b.

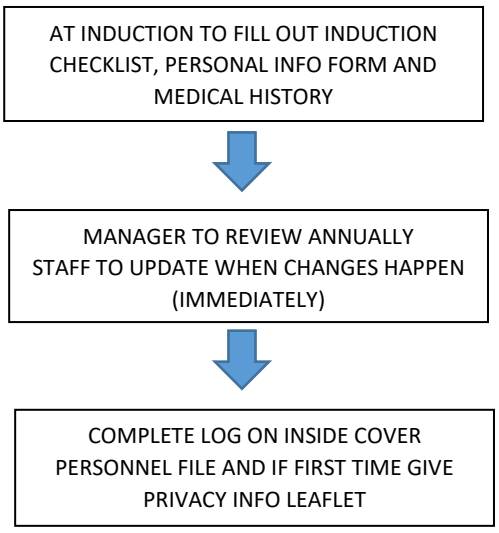
> 11 years computer: leave on Exact and put a note on to say when checked and archived but do not delete

c) Amend any information on patient's record to reflect current dentist etc.
d) Ensure any changes are recorded immediately and accurately
e) 'Paper Trail' the changes
f) Record who we share patient information with**

Staff Information:

a) Do an Information Audit
b) Check for any changes annually but encourage staff to advise of changes throughout the year also
c) Ensure any changes are recorded immediately and accurately
d) 'Paper Trail' the changes
e) Record who we share patient information with**

This process has been mapped out to ensure full understanding of how our duties have changed:



In the instance of destruction of the paper records, we would use the on-site shredder and ensure all parts of the record are destroyed. We would log the destruction in the GDPR file held in reception and only use name and d.o.b as identification of the record which was destroyed. This record will be kept locked away.

In the instance of paper record being archived by being scanned onto the system and then shredded; we will scan the information onto the Exact computer system and then make a note that the paper record was sent for destruction. We will keep the paper record for 48 hours to check that the scanning was a) loaded onto the correct record and, b) that it has been backed up by our backup device. If we have achieved both of these points, then we can shred the paper document.

Who do we share the information with?

We share patient information with very few contacts; other service providers and if requested correctly police or social services. We will only share Information with third parties who have an explicit need for the information – such as a hospital or dental specialist where you need to attend for treatment.

We will get consent prior to sending any referrals. The clinician making the referral will explain the information we need to send (diagnoses, x-rays, medical history list etc.) Once we have consent we will do the referral through our dental program (and if this is not possible we will scan the written referral onto the patient record) and send. With each referral we will send a "received and processing" form which the practice in receipt of the referral will need to return to us to update patient's records and to confirm the safe transit and receipt of the referral. The clinician making the referral will put a note on the patient's record confirming everything they have done, what they have discussed and where the referral is being sent to.

(see point 7 for information on Consent)

3) Communicating Privacy Information

We have produced a leaflet with some "quick look" information for our patients to read and understand and also a Privacy Notice with more information. The Privacy Notice sets out the lawful basis for us processing and using your data. It also informs the patients that they have a right to complain to the ICO if they think there is a problem with how we handle their data.

4) Individuals' Rights

Individuals have very clear rights when it comes to the new GDPR regulations, which includes:

1. The right to be informed – *to know how, when and why we use their information*
2. The right of access - *to be able to request access to their information*
3. The right to rectification – *to be able to request a correction of information we hold*
4. The right to erasure – *to be able to request that their data is erased (if it does not contravene the term we have to keep patient information – 11 years minimum from their last visit)*
5. The right to restrict processing - *to be able to be specific about how they wish their information to be used*
6. The right to data portability – *to be able receive personal data they have provided to a controller in a structured, commonly used and machine readable*
7. The right to object - *to be able object to the processing of their personal data*
8. Rights in relation to automated decision making and profiling – *making a decision solely by automated means without any human involvement; and profiling (automated processing of personal data to evaluate certain things about an individual)*

5) Subject Access Request

Going forward our Subject Access Requests protocols have changed slightly:

- In most cases we cannot charge for complying with a request.
- We now have a month to comply, rather than the current 40 days.

<<We 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.

If we are faced with handling a large number of access requests, we need to consider the logistical implications of having to deal with requests more quickly or having one person on-hand dedicated to dealing with the requests

6) Lawful Basis for processing the data

In order to comply with GDPR we must have a lawful basis for processing information.
Processing shall be lawful only if and to the extent that at least one of the following applies:

1. ***the data subject has given consent to the processing of his or her personal data for one or more specific purposes;***

2. ***processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;***

3. ***processing is necessary for compliance with a legal obligation to which the controller is subject;***

4. ***processing is necessary in order to protect the vital interests of the data subject or of another natural person;***

5. ***processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;***

6. ***Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.***

7) Consent

We have reviewed how we seek, record and manage consent and have made changes. We understand that consent must be freely given, specific, informed and unambiguous, however, as our patients are already in a "business relationship" with us; we may use their information to contact them about special offers, news or changes within the practice. We do not need consent to do this as this falls under "legitimate interest", that is; it is important for us to be able to contact the patients and ensure they are aware of all our services in order that our business can keep earning money. Furthermore, we promote Preventative Dentistry and so it is also important that we are able to keep patients abreast of any new or improved treatments which would help us fulfil this for them.

Consent must be separate from other terms and conditions, and we have introduced simple ways for people to withdraw consent – this is because consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data. We aren't going to refresh all existing DPA consents, but introduce a new format for obtaining consent from now on:

Clinipads:

1) Always check the patient details by accessing the tab when going through the information on clinipads and always ask if the details are up to date, and if not update them.
2) Always check the medical history on every visit

Telephone:

1) Always ask patient to confirm DOB when accessing their record
2) If there is a note on the system that a relative/friend etc. is able to discuss their account, get a specific name of whom, and tell them we will ask the third party to confirm their DOB when they call or come in. Update the system to reflect you checked putting the date and your initials

Face to Face:

1) Always check you are speaking to patient – if the date looks too old or young, male or female etc.
2) If possible ask patient to confirm DOB

8) Children

Fortunately through the NHS FP17's we have a process in place where we can check a person's age. If a patient is joining us as a private patient there is no provision for checking age, so from now on if someone is wanting to join our practice and looks young, we will ask for verification of age as if under age, we need to obtain parental or guardian consent for any data processing activity.

The introduction of the GDPR brings in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. Our website contains forms which can be filled in by a person without asking the age, however by 25th May 2018 we will include age identification tabs and information as to why we need them on each website. 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'.

9) Data Breaches

We have ensured we have the right procedures in place to detect, report and investigate a personal data breach. We are already required to notify the ICO (and possibly some other bodies) if we suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. We 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.

If we identify an area which could potentially suffer a Data Breach, we must report it immediately to the DPO for the site via the forms provided

10) Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'.

It also makes DPIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

Where we are inputting all the patient records from paper onto the computer program, this requires a DPIA because it is a situation where data processing is likely to result in high risk to individuals, for example:

- Where a new technology is being deployed;
- Where a profiling operation is likely to significantly affect individuals; or
- Where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and we cannot sufficiently address those risks, we would be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR. Fortunately in this situation the risk has been deemed very low and so we will not be required to report this

10) Data Protection Officer – DPO

As a dental practice, we have a DPO and here at Sandes Avenue Dental Practice; Kerry Healey is to take responsibility for data protection compliance within our practice and her title will be Data Protection Officer

Review date: May 2019

Next Review: May 2020