Dental Protection

The General Data Protection Regulations 2018

Practicalities for Practice

Martin Foster
Dento-Legal Adviser

The Background

The legislation

- EU Directive on Data Protection

- EU General Data Protection Regulation (GDPR)
- In force from **25 May 2018 – 8 weeks & 6 days to go** ….

GDPR aims

- Enhance current data protection rules
- Additional data protection obligations for organisations
- Increased rights for individuals.

- If organisation is complying with the current law then will be well on the way to compliance with GDPR …but
- Much greater emphasis on documentation
- Data controllers must be able to demonstrate compliance

GDPR - Principles

1. **Lawfulness**, **fairness** and **transparency**

2. **Purpose limitation** - data collected only for specified purposes.

3. **Data minimisation** – adequate & limited to what is necessary

4. **Accuracy** - up to date

5. **Storage limitation** - kept for no longer than is necessary

6. **Integrity & confidentiality** – protect from unlawful processing / loss

7. **Accountability** – demonstrate compliance

GDPR affects

Data **'Controllers'** and **'Processors'**

- **Controller** determines the purposes / means of processing data.
- P**rocessor** is responsible for processing on behalf of a controller.

- **Obligations of a Controller**
  - Ensure processors comply with GDPR

- **Obligations of a Processor**
  - Maintain records of personal data and processing activities
  - Legal liability if responsible for a breach

GDPR Definition of "Personal Data"

'Personal Data' = **information** relating to a **"data subject"**

A data subject is:

1. an **identified** or
2. an **identifiable** natural person

An identifiable "natural" person is one who can be identified, directly or indirectly, by a unique identifier

e.g. *name, ID number, location data, IP address, or factors specific to the identity of that person.*

Lawful processing - Consent

Consent Under GDPR

Where consent is the basis relied upon for processing, the requirement is for consent to be "unambiguous" and "explicit" .

Consent must be freely given, specific, informed and a clear indication of the individual's wishes

Lawful processing - Consent

What's new?

- GDPR sets a high standard for consent
- Consent must be unambiguous - clear affirmative action
- Pre-ticked opt ins are banned

- Silence does not constitute consent under the GDPR
- Consent must have clear record of how and when given

- Individuals have the right to withdraw consent at any time
- There are new provisions regarding children's personal data

GDPR – Consent

Obtaining & recording consent?

Request should be clear, concise, separate from other Terms & Conditions and easy to understand:

Request should include:

- organisation name;
- name of any third parties who will rely on the consent;
- why the data is sought;
- what will be done with the data; and
- the fact that the patient can withdraw consent at any time.

GDPR – Patient's rights

- Transparency
- Subject Access
- Rectification
- Erasure
- Restriction
- Data portability
- Objection
- Profiling

GDPR – Accountability Principle

- The GDPR promotes **accountability** and **good governance**

- Organisations will have comprehensive governance
- More policies & procedures for practices
- Should minimise risk of breach
- Protect personal data comprehensively

GDPR – Retention

- Personal data should be retained for **no longer than is necessary** for the purposes for which it is processed
- Requirement to inform data subject of proposed retention period/criteria used to determine period
- Consider job applications/ex-employees' data
- Consider retention policy in place/diarise review

GDPR – Demonstrating Compliance

Strict obligations on controllers **and** processors.

Processors now accountable for their actions

No longer sole responsibility of controller

Demonstration of **compliance with principles**.

GDPR – Demonstrating Compliance

The controller **must**:

- Implement measures/demonstrate compliance
- Maintain relevant documentation on processing
- If required, appoint a data protection officer
- Implement measures to meet principles of data protection
- Use “data impact assessments” where necessary

GDPR - Security Principle

Appropriate security measures in place to prevent unlawful / unauthorised processing and loss of personal data.

Security of personal data from the **point of collection** to the **point of destruction.**

Entrance security, lockable cupboards/ drawers, screen locking, secure disposal methods, encryption , “cloud” computing.

GDPR - Data Security Breaches

Breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data Protection Commissioner must be notified if breach likely to result in a **risk to the rights and freedoms** of individuals.

Evaluate whether the breach will have a significant detrimental effect on individuals (discrimination, damage to reputation, financial loss or loss of confidentiality.)

In addition to **fines**, data subjects may apply to the courts for **compensation** if they have suffered from loss.

GDPR - Monetary Penalties

Under the **GDPR**, penalties for breach & non-compliance are significantly increased.

The position is that fines must **punish** and not just deter.

Tier 1 infringements – fine of up to 2% of annual turnover or 10 million euros (whichever is higher)

Tier 2 infringements equate to a fine of up to 4% of annual turnover or 20 million euros (whichever is higher)

GDPR - Subject Access Requests

Now more onerous:

- No charge from 25 May 2018
- The time to provide the data reduced to one month
- If request unreasonable/ excessive can levy charge or refuse
- You should verify the identity of the person making the request by “reasonable means”
- You should inform the person making the request of their rights

So what does this all mean for my practice ?

?

The General Data Protection Regulations and your Practice.

Friday 25th May 2018 is “GDPR” day.

The new law recognises the digital age and is designed to deal with this.

Practices have to get to grips with this

In practical terms …..

All “data controllers” and “data processors” are affected, so 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 the DPC website.

Data Processing

Processing data - includes collecting, storing, using, disclosing (and destroying) personal information e.g. dental records / staff records.

- There must be a “legal basis” (i.e valid reason) for holding personal information **and**
- This legal basis is made clear to patients.

Data Processing

In dental practice the relevant legal basis will be that the “data processing” is necessary for the provision of treatment by a registered dental professional.

- duty of confidentiality is “fitted as standard”

Another basis is the consent of the patient consent to the processing of his/her data.

Data processing - consent

- Agreement to data processing must be based upon an accurate understanding of the reason for the processing,
- The patient has freedom to choose
- The information is used only for a specific purpose.

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,

Essential that there is clear documentation of patient consent for his/her information to be used.

Transparency & Fair Processing

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.

“Privacy notice”

Should contain :

- Who the data controller is 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 patient must be advised of rights.

(including advice on complaining to DPC if concerns)

Patient rights

- A patient has the right to be provided with copies of the information held within 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.

More Patient rights

Patients have greater rights regarding rectifying and erasing records and with restricting processing.

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 within the timeframe.

Data breach

If there is a breach of patient confidentiality, the data controller must notify the DPC without delay

If possible within 72 hours of becoming aware.

The patient must also be informed if the breach has a high risk of affecting his/her privacy rights.

The new regulations provide for higher penalties for data breaches.

Data Protection Impact Assessment

Assessments are a means of demonstrating the measures in place to safeguard patient information.

These assessments are required if the way in which information is handled has the potential to breach confidentiality.

For example, installation of new patient record software or a new system for sharing information or making referrals.

Important to document “assessments” of practice systems

(Think of it as audit)

Data Protection Officer

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

At present it would appear that hospitals, managed services, large multi-clinics or chains of practices would require a DPO but an individual practitioner would not.

Where the line is drawn however is not specified although the number of individuals for whom information is held will clearly be a major factor.

Data Protection Officer required ?

If any doubt about need for a DPO, until clarification is available it would be advisable to carry out a self- assessment of your own practice in terms of the personal data held. Remember it includes patients *and staff*.

Advice can be sought from the DPC

The conclusion of any assessment should be documented giving the reasons whether or not a DPO was considered necessary.

This will **demonstrate** that steps were taken to ensure compliance with the regulations.

Data Protection Officer Role

If a DPO is appointed, the role is to monitoring and advise on the practice's compliance with data protection requirements.

This includes pointing out if something is not as it should be

The role cannot be discharged by the same person who is responsible for data protection measures in the practice.

The DPC has helpful guidance relevant to the appointment of a DPO at :

https://www.dataprotection.ie

Things to do

Ensure that you keep up to date with the updates from the Data Protection Commissioner.

https://www.dataprotection.ie/docs/GDPR/1623.htm

http://gdprandyou.ie/

Drink coffee and write a to-do list

Document

- the nature of all personal data held
- how it is collected
- how it is stored
- who has access
- who it is shared with

Three more things to check…

Ensure there is a legal basis for processing data.

If based upon consent there must be an appropriate system in place for recording this.

Ensure “privacy notices” comply with the GDPR.

Decide if a DPO is required. If so ensure he/she has appropriate knowledge.

Another three….

- Be able to provide copies of patient records promptly and in an appropriate format
- Have a clear procedure for reporting data breaches to the DPC.
- Make sure that all staff are aware of what the GDPR means.

Take home message

Practices need to be completely open and transparent about why personal data is collected and what it is used for.

It is necessary to clearly demonstrate how data is processed & protected.

For further information visit

www.dentalprotection.org