Brixham Dental Practice

Data Protection Overview

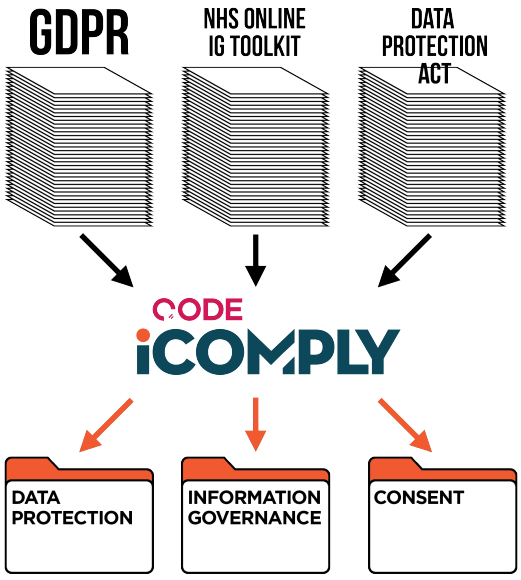
- The General Data Protection Regulation (GDPR) becomes law on the 25th May 2018. The main changes under the GDPR are new compliance obligations for data controllers and processors
- The Government has announced a new Data Protection bill, to sign the European GDPR regulation into law and to update the Data Protection Act. The details of the new Act are as yet unclear, there may be special provisions for health records
- This overview should be read in conjunction with Information Governance Procedures (M 217C). See the Data Protection and Information Security Policy (M 233-DPT) for all related templates.
- Every data controller must register with the ICO. See below to identify who are the data controllers
- Processing of data includes collecting, recording, using, organising, storing, changing, viewing, modifying, publishing, and deleting or destroying it
- It is important to note that there are other data regulations such as ePrivacy which apply to marketing. ePrivacy is being updated and at the time of writing it has not been published
- The first time you set up GDPR compliance use the latest GDPR and Data Protection Action Plan (M 216A)
- This Overview and its related templates may be updated, if required when the Data Protection Act and ePrivacy regulation have been released and the ICO have updated their guidance

Data protection compliance

For dental practices the compliance is complex, we have to take into account consent for treatment, health records which is the processing of sensitive category data, consent for marketing to both patients and non-patients, which is the processing of personal data plus managing personnel files which could include both types of data. To add complexity NHS practices also have to complete the online IG toolkit, which has its own terminology and requirements. The Information Commissioner website provides its interpretation of the legislation and how you should meet data protection requirements, it's a useful resource and is being updated frequently.

CODE iComply manages the data protection complexity by allocating its requirements into three areas:

- Data Protection (M 216) – this provides an overview of all data processing requirements including the Data Protection Act (DPA), the GDPR and the CODE Data Protection and Information Security Policy (M 233-DPT)
- Information Governance – which provides the procedures, policies and risk assessments to meet the DPA, NHS and GDPR requirements in a format that can be used for the NHS IG Online Toolkit. The templates range from (M 217) to (M 217UA)
- Consent – covers all aspects of consent and patient confidentiality including Valid Consent for treatment (M 292), Information Governance Procedures (M 217C), Communication Consent Form (M 217RA), Consent for Clinical Photography (M 217RB), Data Requests Record (M 217RX) and Confidentiality Policy (M 233-CON)



Information Governance
The CODE definition of Information Governance brings together the requirements to meet the Data Protection Act, the General Data Protection Regulation (GDPR), patient consent, privacy, information security, record keeping, confidentiality, computer security, internet security, NHS requirements, record keeping requirements and others. The Information Governance templates have also been designed to assist with completion of the NHS online IG Toolkit.

Key data protection principles under the GDPR

Penalties
Under GDPR organisations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).

Consent
Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it. Consent must be opt-in and not 'tick to opt out', also it must be granular so that the person can see exactly what they are consenting for.

Breach Notification
Breach notification will be mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access
This is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge.

Right to be Forgotten
Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

Data Portability
GDPR introduces data portability - the right for a data subject to receive the personal data concerning them in a '*commonly use and machine readable format*', Data Portability is primarily for the large social media companies.

Privacy by Design
Privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - *'The controller shall implement appropriate technical and organisational measures in an effective way in order to meet the requirements of this Regulation and protect the rights of data subjects*'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officer
A Data Protection Officer (DPO) is required for all public authorities, [in practices that provide NHS treatment the DPO is the Information Governance Lead][in private only practices, there is no requirement to have a DPO as we do not process large amounts of personal data].

Who is the data controller?
A data controller must register with the ICO. The data controller is **responsible** for the processing of data. A data controller is an individual, a partnership, a company etc. When deciding who in a practice is the data controller you can refer to the ICO research : "Information Governance in Dental Practices", which says:

> *"1. Are you responsible for the control and security of patient records, and do you have other responsibilities associated with the data?*
> *2. Do you have a patient list separately from the practice in which you treat patients; that would follow you if you left?*
> *3. Do you treat the same patient at different practices?*
> *4. If a complaint was made by a patient, or data was lost, would you be legally responsible for dealing with the matter?*
>
> *If you answer 'yes' to any of the above questions, you are likely to be a data controller and will need to register with the ICO."*

The "data processor" means any person or company (other than an employee of the data controller) who processes the data on behalf of the data controller. This could be a third-party company such as a cloud storage company used for backup of patient records.

CODE has interpreted that the guidance requires:

- Single-handed practice owners to register as individuals and their registration will cover all team members
- Partnerships to either have one registration under the partnership name or, if each partner has his/her own patients, a separate registration for each partner is needed
- Expense sharing partners and self-employed associates/hygienists/therapists to register and pay the fee individually
- A limited company with a number of practices to have one registration if the company has group policies and procedures that determine why and how personal data is used
- If you own a practice as an individual but also have a limited company for tax purposes, to have an individual registration with ICO

See the Information Commissioner's Office registration link. The cost of registration is £35. Each registration entry is valid for one year and reminders are sent when renewal is due.

Changes to the ICO register
Any changes to the register (including the name, address, practice or intentions in respect of data processing and changes to security measures) must be notified within 28 days from the event. Changes involving new processing must be notified before it starts. Although changes to personal details are free, changes to the registration entry from associate to practice owner will be viewed as a new entry and will incur another £35 fee.

Data types – personal and special category
Personal data means data which relates to a living individual who can be identified:

- From the data, or
- From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller
- Including any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Special category data includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership;
- Data concerning health or sex life and sexual orientation;
- Genetic data
- Biometric data where processed to uniquely identify a person

Legal basis for processing personal data
GDPR require you to identify a legal basis to process personal data. There are six options, they have equal importance as no option is preferable to any other:

1. Consent of the data subject
2. Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
3. Processing is necessary for compliance with a legal obligation
4. Processing is necessary to protect the vital interests of a data subject or another 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. Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.)

The legal basis for processing *special category data* in a dental/medical practice includes:

- *"9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional."*

Examples of the legal basis for processing *personal data* could be:

- Consent of the data subject
- Necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Necessary for the purposes of legitimate Interests pursued by the controller or a third party

Examples of processing personal data could include personnel files, email details of a non-patient for marketing and marketing to patients.

Consent
An important aspect of the GDPR is the requirement to offer people choice and control over how their data is used. For clinical records there is a legal basis for processing special category data. But if you are sending out email newsletters for example, you may need to consider the consent requirements, such as:

- The consent form gives choice about the how the data will be used e.g.to provide news/advice/ important announcements/new products and services
- The consent statement must be clear and specific, and the indication to give consent must be unambiguous
- Tick boxes must never be pre-ticked, this is called 'positive opt-in'
- Consent must be easy to withdraw with a clear way to withdraw it at any time such as by phone or email
- Evidence of consent is kept, including who, when, how, and what you told people
- The consent process is kept under review, and refreshed if anything changes, it is reviewed annually in iComply

For patient consent procedures see Valid Consent (M 292).

Legitimate interests
The Data Protection Network provides some useful information about how legitimate interests may be used as a lawful basis to carry out marketing. CODE cannot advise on this as the legal issues are too complex and there is no official guidance yet. For business-to-consumer marketing members will have to take into account ePrivacy legislation and the new Data Protection Act. There is a template Legitimate Interests Assessment (M 217S) if you want to explore this legal basis, perhaps for direct mail or other non-electronic marketing activities.

Data Breach Notification
See Information Governance Procedures (M 217C).

Right to Access
Individuals have the right to obtain:

- Confirmation that their data is being processed
- Access to their personal data
- Other supplementary information – this largely corresponds to the information that should be provided in a Privacy Notice (M 217T)
- Information must be provided without delay and at the latest within one month of receipt, this can be extended under certain circumstances

Patients have the right to access a copy of their clinical records and receive a free copy, non-patients can request a free copy of the details that you hold on file for them. The details must be provided within a month of the request. You should refer individuals wishing to make a request to your Data Protection Policy (M 233-DPT).

See Information Governance Procedures (M 217C) for more information about Right to Access.

Privacy Impact Assessments
Privacy impact assessments (PIAs) help practices to identify the most effective way to comply with the obligations of the GDPR. The assessment sets out the options for addressing each identified risk and whether the options for addressing the result in the risk being:

- Eliminated
- Reduced or
- Accepted

The Privacy Impact Assessment in the updated Sensitive Information Map, PIA and Risk Assessment (M 217Q).

The right to be forgotten
Patients will be able to ask businesses and organisations for access to their personal data and for it to be wiped, giving them more control over how their information is removed. However, it is currently unclear how this will apply to medical records that may be exempt.
The new UK law will require social media companies to delete all of a person's posts from before they were under 18, if they ask for it.

Further information
The IG toolkit can be found at www.connectingforhealth.nhs.uk/systemsandservices/infogov
Information Commissioner's Website fond at www.ico.org.uk
Data Protection Network www.dpnetwork.org.uk/dpn-legitimate-interests-guidance