Bletchley Dental Practice

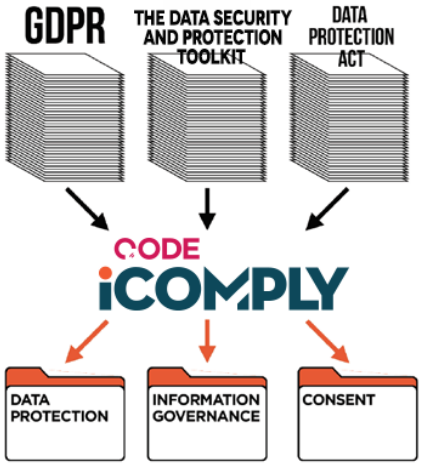
Data Protection Overview

- The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 are now law. The main changes are new compliance obligations for data controllers and processors
- CODE uses the term "information governance" to include GDPR, data protection and information security
- This overview should be read in conjunction with the the Data Protection and Information Security Policy (M 233-DPT), it lists related policies, procedures, risk assessments and other 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
- Use the latest version of the GDPR and Data Protection Action Plan (M 216A) to see what has changed and what you need to do
- The CODE information governance policies, procedures and risk assessments are liable to change as the ICO interprets the Data Protection Act 2018 and provides us with guidelines. We also learn as the profession in general gains an understanding of proportionate compliance and national requirements are tweaked for dentists. The current iComply templates will be updated periodically to keep you on track

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 special 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 Data Security and Protection 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 Data Security and Protection 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)



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."*

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 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
- Self-employed associates/hygienists/therapists can either register individually and be joint data controllers or not register and be processors. Note that in either situation they will need to sign the Model Contract for Data Processor or Joint Data Controllers (M 217UA)

CODE always looks at regulations and requirements situations differently because we understand the business of dentistry, we always plan to reduce risk to practice owners and managers as much as possible. The new cost of registering is just £40 so it's a negligible cost and administration. Practice owners may consider asking their self-employed associates/hygienists/therapists to register individually with the ICO. This was our stance in the past and we still recommend it but no longer say it is obligatory.

See the Information Commissioner's Office registration link. Each registration entry is valid for one year

and reminders are sent when renewal is due.

Data processor
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. Here are some examples:

- Dental laboratories
- Self-employed clinicians (unless they register with the ICO individually)
- Google (if you use adwords, captcha or analytics etc)
- Microsoft – if you use office 365 or other cloud services
- Dropbox
- Online backup company
- Online HR app like the CODE Total HR App
- Your computer and network support company if they can access your data
- Your patient management software company if they have a cloud aspect

Information Governance
The CODE definition of Information Governance brings together the requirements to meet the Data Protection Act 2018, the General Data Protection Regulation (GDPR), patient consent, privacy, information security, record retention, 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 Data Security and Protection Toolkit.

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

> *"We pride ourselves on being a fair and proportionate regulator and this will continue under the GDPR. Those who self-report, who engage with us to resolve issues and who can demonstrate effective accountability arrangements can expect this to be taken into account when we consider any regulatory action."*

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. In dentistry, with the CODE GDPR approach, consent relates primarily to marketing and criminal record checks.

Breach Notification
Breach notification is mandatory 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. See the notification procedure in Information Governance Procedures (M 217C).

Data rights of the individual
Under GDPR, the individual has data privacy rights which must be stated in your Privacy Notice (M 217T). The procedure for managing privacy rights is in Information Governance Procedures (M 217C).

The right to be informed
Individuals have the right to be informed about the collection and use of their personal data

The right of access

Individuals have the right to access their personal data (this was called subject access request). Patients have the right to access a copy of their clinical records and receive it free, 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 Privacy Notice (M 217T) and provide a copy if required.

The right to rectification
The right for individuals to have inaccurate personal data rectified, or completed if it is incomplete

The right to erasure
The right for individuals to have personal data erased. CODE suggests that clinical records must be retained for the retention periods in Record Retention (M 215)

The right to restrict processing
To request the restriction or suppression of their personal data. See above about clinical records. But if a patient leaves the practice, they can request that you no longer process their data.

The right to data portability
To obtain and reuse their personal data for their own purposes. For example transfer a copy of patient records to another practice.

The right to object
To object to the processing of personal data.

Rights in relation to automated decision making and profiling
Where a decision is made solely by automated means without any human involvement

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, which include dental practices who provide NHS treatment. The regulations state that DPOs should be experts in the field, which seems implausible for individual dental practices. Recently ministers have refused to make exemptions of this requirement for small NHS providers. It is CODE's suggestion that the Information Governance Lead takes on the role of Data Protection Officer for the time being and see how the situation unfolds. The only other practical solution would be to engage a consultant to fill the role, but they may be difficult to find and expensive.

Establishing a legal basis for processing data
There are two types of data, personal data and special category data. You must establish legal bases for processing each type:

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 bases for processing 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 to provide dental treatment
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

Examples of the legal basis for processing personal data in a dental practice could be:

- Necessary for the purposes of legitimate Interests pursued by the controller
- Necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Consent of the data subject
- Processing is necessary for compliance with a legal obligation to which the controller is subject

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

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

- The legitimate interests of the controller
- Necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- For health and social care services
- Consent of the data subject (including for criminal record checks)

The legal bases you decide upon should be entered into your Privacy Notice (M 217T).

Consent
An important aspect of the GDPR is the requirement to offer people choice and control over how their data is used. For dental care we have established the legal basis for processing special category data. But if you are sending out email newsletters for example, you may need to consider 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 ICO says:

> *"The legitimate interests basis is likely to be most useful where there is either a minimal Legitimate interests is the most flexible of the six lawful bases. It is not focused on a particular purpose and therefore gives you more scope to potentially rely on it in many different circumstances.*
> *It may be the most appropriate basis when:*
>
> - *The processing is not required by law but is of a clear benefit to you or others*
> - *There's a limited privacy impact on the individual*
> - *The individual should reasonably expect you to use their data in that way; and*
> - *You cannot, or do not want to, give the individual full upfront control (ie consent) or bother them with disruptive consent requests when they are unlikely to object to the processing*
> - *There may also be occasions when you have a compelling justification for the processing which may mean that a more intrusive impact on the individual can be warranted. However in such cases you need to ensure that you can demonstrate that any impact is justified*
> - *Impact on the individual, or else a compelling justification for the processing"*

CODE has suggested legitimate interests as a basis for processing patient's personal data. This will be reviewed when the ICO provide guidance on the new Data Protection Act 2018. To apply legitimate interests you must perform a Legitimate Interests Assessment. You can adopt the first template assessment in Legitimate Interests Assessment (M 217S), remember to remove the second marketing template assessment before you adopt this document.

Note that the second legitimate interests assessment template in (M 217S) is for marketing, but this is only provided for information. CODE cannot provide advice on using legitimate interests for marketing until there is further guidance.

The Data Protection Network provides some useful information about how legitimate interests may be used as a lawful basis to carry out marketing. For business-to-consumer marketing members will have to take into account ePrivacy legislation and the new Data Protection Act.

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

In the GDPR and Data Protection Action Plan (M 216A) you are prompted to carry out the he Privacy Impact Assessment in Sensitive Information Map, PIA and Risk Assessment (M 217Q).

Online Toolkit
The NHS Information Governance online toolkit has been replaced by the Data Security and Protection Toolkit. From July 2018 you will be able to use the updated IG Improvement Plan (M 217A) to simplify completion of the new online toolkit. Note that this is only necessary for practices who provide NHS treatment.

What to do next

- Follow the GDPR and Data Protection Action Plan (M 216A).
- Keep an eye on iComply news for any changes when the Data Protection Act advice is available from the ICO as there will be further updates from CODE

Related templates
For a full list of related templates see the Data Protection and Information Security Policy (M 233-DPT).

Further information

Information Commissioner's Website found at www.ico.org.uk
Data Protection Network www.dpnetwork.org.uk/dpn-legitimate-interests-guidance
The Data Security and Protection Toolkit https://www.dsptoolkit.nhs.uk/