Data Protection Overview

This overview gives a general guide and should be read in conjunction with the Data Protection and Information Security Policy (M 233-DPT) to help ensure that your practice conforms to UK GDPR and the Data Protection Act 2018.

This overview covers:

- The Agilio approach to 'Information Governance'
- Who should be a data controller and how to register with the information Commissioner's Office (ICO)
- The processing of data including collecting, recording, organising, storing, changing, viewing modifying, publishing, and deleting or destroying it
- The data rights of individuals
- What an Information Governance Lead is and who should be appointed
- If NHS, what a Data Protection Officer (DPO) is and who should be appointed
- The legal bases that must be specified for data processing
- What legitimate interests are and how it applies in your practice
- If NHS, what is and how to comply with the national data opt out policy
- Data transfers within and outside the EU

Please note, throughout this document, the term "information governance" refers to GDPR, data protection and information security.

Data protection compliance

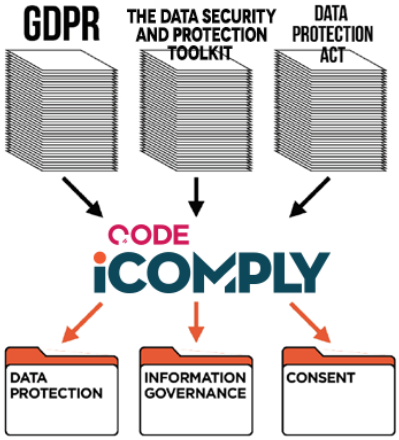
For dental practices the compliance is complex, we have to take into account the processing of special category data, consent for marketing to both patients and non-patients, which is the processing of personal data plus managing personnel files which could include both types of data. To add complexity 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.

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 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 UK GDPR requirements in a format that can be used for the Data Security and Protection toolkit. The templates range from (M 217) to (M 217X)

- **Consent** – covers all aspects of consent and patient confidentiality including, 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?
Every organisation or sole trader who processes personal information needs to pay a fee to the ICO, unless they are exempt. 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 guidance which says that you should ask who decides:

- to collect personal data in the first place
- the lawful basis for doing so
- what types of personal data to collect
- the purpose or purposes the data are to be used for
- which individuals to collect data about
- whether to disclose the data, and if so, to whom
- what to tell individuals about the processing
- how to respond to requests made in line with individuals' rights, and
- how long to retain the data or whether to make non-routine amendments to the data

These are all decisions that can only be taken by the controller as part of its overall control of the data processing operation. If you make any of these decisions determining the purposes and means of the processing, you are a controller.

We have 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 will either be joint-controllers or processors and will need to sign the Model Contract for Data Processor or Joint Data Controllers (M 217UA)

Agilio 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 cost of registering starts at just £35 and practice owners may consider asking their self-employed associates/hygienists/therapists to register individually with the ICO if it has been determined that they are data controllers. 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 Agilio iTeam 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 Agilio definition of Information Governance brings together the requirements to meet the Data Protection Act 2018, the UK General Data Protection Regulation (GDPR), marketing 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 UK GDPR organisations in breach of the regulation can be fined up to 4% of annual global turnover or £17.5 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. In dentistry, with the Agilio 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 UK 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. Agilio 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. It is Agilio's suggestion that the Information Governance Lead takes on the role of Data Protection Officer, unless this role is held by the practice owner (in which case it should be the practice manager). The only other practical solution would be to engage a third party, this could be 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 activities related to each type and specify additional appropriate 'conditions' for processing special category data:

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

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

The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data
- biometric data (where used for identification purposes)
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation

Article 9 of UK GDPR lists these appropriate conditions for processing special category data:

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law)

The legal bases you decide, along with Article 9 conditions for processing special category data, should be entered into your Privacy Notice (M 217T). We have provided templated examples on the document.

Consent
An important aspect of the UK GDPR is the requirement to offer people choice and control over how their data is used. For dental care we have established the legal bases and appropriate conditions 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

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"

To apply legitimate interests, it is highly recommended you 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. Agilio 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 The Privacy and Electronic Communications Regulations and the Data Protection Act 2018. A dental practice may also consider legitimate interests a legal basis for processing when undertaking the safe transfer of paper records to a secure digital patient records system.

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

Online Toolkit
The Data Security and Protection Toolkit is an online self-assessment tool that is updated each year to reflect the latest data protection thinking. All organisations that have access to NHS patient data and systems, including private practices with NHSmail accounts, must use this toolkit annually to provide assurance that they are practising good data security and that personal information is handled correctly.

You can use the latest Guide for Completing the Data Security and Protection Toolkit (M 217A) to simplify completion of the online DSP toolkit each year.

Data Opt Outs
All NHS health and care organisations in England must comply with the national data opt-out policy. The data opt out does not apply to health or care services which are accessed within Scotland, Wales or Northern Ireland.
Most dental practices will not be using patient data for research or audits.

The national data opt-out applies to "confidential patient information" (CPI) and guidance is provided for health care professionals in assessing what is CPI for the purposes of applying the national data opt-out.

Confidential patient information is broadly:

- Identifiable or likely identifiable e.g. from other data likely to be in the possession of the data recipient; and
- Given in circumstances where the individual is owed an obligation of confidence; and
- Conveys some information about the physical or mental health or condition of an individual, a diagnosis of their condition; and/or their care or treatment

The term confidential patient information (CPI) also covers data which falls within the "special categories of personal data" under article 9 of UK GDPR. This means that practices are expected to continue to apply data opt-outs for an individual after they have died.

Purposes beyond direct care includes audits and research e.g. for:

- Improving the quality and standards of care provided
- Research into the development of new treatments
- Preventing illness and diseases
- Monitoring safety
- Planning services

Any person with an NHS number allocated to them is able to set a national data opt-out. This covers the majority of patients who have received health or care services in England and, therefore, have data about them in the health and care system in England.

A child is able to set their own opt-out from age 13, which aligns with the minimum age at which children can give their consent to participate in digital services as set out in data protection legislation. This is not based on any test of competence. Children under 13 and those who lack capacity are not able to set an opt-out themselves. In these cases, individuals who have a formal legal relationship to act on behalf of them (i.e. somebody who has parental responsibility, a lasting power of attorney or court appointed deputy) are able to set an opt-out on their behalf by proxy.

A number of different channels are available for the public to set a national data opt-out. These are:

- A digital (online) channel accessed via the national data opt-out service.
- For those who need support to set their national data opt-out preference online a digitally-assisted channel is provided that enables members of the public to set a national data opt-out with assistance from NHS Digital staff via the national helpline
- A non-digital (paper based) channel accessed by the national helpline or through forms which can be printed from the webpages, and
- Via the NHS App

Depending on the situation, an individual may be restricted to certain channels (i.e. Those with parental responsibility wishing to opt out on behalf of a child under 13 years of age can only do so via the non-digital channel). Further information can be found on page 16 of the NHS National Data Opt-out Operational Policy Guidance Document.

For clarity the national data opt-out is for patient data only and applies to confidential patient information - the national data opt-out does not apply to workforce or staff data.

If you are planning to use confidential patient information for purposes other than their direct care, NHS Digital has developed a technical service where you can check NHS numbers. See below for the link.

This service can be used in two ways:

1. Organisations can submit a list of NHS numbers that they need to disclose and the service looks these up against the central repository of national data opt-outs. It returns a "cleaned list" of those that do not have a national data opt-out i.e. it removes the NHS numbers for those with a national data opt-out. This is most suitable for one-off and infrequent disclosures of data.

2. Organisations can submit the NHS numbers for all patients with whom they have a legitimate relationship and then store temporarily the list of patients who do not have an opt-out at the current time and whose data they may be able to disclose. (Organisations would still need to have the appropriate legal basis for any such disclosures. This must not be interpreted as, or confused with, a patient's explicit consent to the sharing of their data.) There are a number of policy rules around the storage and use of this "temporary cache" of data which are set out below. This is most suitable for large scale and frequent disclosures of data.

People can continue to be able to give their explicit consent separately if they wish, e.g. to be involved in research, as they do now. They should be able to do so regardless of whether they have opted out of their data being used for purposes beyond direct care. This should apply to patients' decisions made both before and after the implementation of the new opt-out model.

Further information on Data Opt Out
For guidance on whether the Data Opt Out policy does or does not apply to a disclosure see the National data opt-out operational policy guidance document
NHS Digital technical service which enables health and adult social care organisations to check if their patients have a national data opt-out
Patients can view or change their national data opt-out choice at any time by using the online service at www.nhs.uk/your-nhs-data-matters

UK GDPR, Brexit and International Transfers/Processing
UK GDPR stands for the UK General Data Protection Regulation. It is a UK law which came into effect on 01 January 2021 and is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679) which applied in the UK before that date. UK GDPR and GDPR are practically identical when it comes to managing data protection in a dental practice environment, though may diverge in the future.

In 2021 the EU decided that UK GDPR was 'adequate' and therefore most data can continue to flow between the UK and the EU/EEA without the need for additional safeguards required for international transfers (see below)

The UK government now has the power to make its own 'adequacy decisions' in relation to international transfers/organisations known as 'adequacy regulations'. These are regulations put in place to state that the data protection regime of a named country has reached the required standards of UK GDPR. If practices wish to transfer data/have data processed outside of the UK/EU then one of the first step is to check if there is an adequacy regulation in place for that country.

There are provisions to allow the continued use of any EU Standard Contractual Clauses ('SCCs'), and pre-

existing Binding Corporate Rules to transition into the UK data protection regime. However new SCCs will be introduced in 2022 and practices should check ICO guidance if wishing to transfer data/have data processed outside of the UK/EU.

Digital data stored and processed in the USA
The European Court of Justice have held that the Privacy Shield is no longer a valid way to transfer personal data outside of the European Economic Area (which includes the UK). This case is known as Schrems II. As a result of this you should now review all your processing agreements following the steps below. Agilio recommends you try to limit the transfer of data to within the UK or EU wherever possible.

All practices should follow the steps below where you have identified that data is processes or stores your data in the US.

Step 1
Consider whether any changes could be made so the data stays within the UK or EU. To do this, you should contact your processor to discuss a solution (for example, their agreement that your data will remain within the UK or EU). For big companies such as Dropbox or Microsoft you may find that there is a tool to make this switch within the admin account settings.

If this is not possible, continue to Step 2.

Step 2
If the transfers to the US must continue, the practice are required to undertake an assessment to identify whether a transfer mechanism, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), provides enough protection for each data transfer. This can be recorded simply on a word document. See the section below on 'Digital data stored and processed outside of the UK/EU' for more information on the process to follow.

Large companies which rely on data being transferred from the UK and/or EU to the US will often have these mechanisms clearly stated within their Privacy Policy. For example, Invisalign provide a link to their Binding Corporate Rules which demonstrate how they undertake these data transfers and comply with EU law. You should always review any mechanisms to ensure that you, as the controller, are satisfied that the measures in place to protect your data subjects' information

Data stored and processed outside of the UK/EU
It is generally not recommended to transfer data outside of the UK/EU. Refer to the ICO's page on International transfers after the UK exit from the EU Implementation Period for the latest guidance. At the time of this update the guidance is to follow this checklist:

1. **Are we planning to make a restricted transfer of personal data outside of the UK?**
   If no, you can make the transfer. If yes, go to Q2
2. **Do we need to make a restricted transfer of personal data in order to meet our purposes?**
   If no, you can make the transfer without any personal data. If yes, go to Q3
3. **Are there UK 'adequacy regulations' in relation to the country or territory where the receiver is located or a sector which covers the receiver (which currently includes countries in the EEA and countries, territories or sectors covered by existing EU 'adequacy decisions')?**
   If yes, you can make the transfer. If no, go to Q4
4. **Are we putting in place one of the 'appropriate safeguards' referred to in the UK GDPR?**
   If yes, go to Q5. If no, go to Q6
5. **Having undertaken a risk assessment, we are satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime.**

If yes, you can make the transfer. If no, go to Q6.

6. Does an exception provided for in the UK GDPR apply?

If yes, you can make the transfer. If no, you cannot make the transfer in accordance with the UK GDPR

If you reach the end without finding a provision which permits the restricted transfer, you will be unable to make that restricted transfer in accordance with the UK GDPR.

You can see that in order to transfer data outside of the UK/EU you must perform a written assessment and ensure that adequacy regulations or appropriate safeguards are in place.

Appropriate safeguards include:

A legally binding and enforceable instrument between public authorities or bodies

- Binding Corporate Rules (BCRs)
- Standard contractual clauses (SCCs)
- An approved code of conduct
- Certification under an approved certification scheme
- Contractual clauses authorised by the ICO
- Administrative arrangements between public authorities or bodies

Refer to the ICO's page on International transfers after the UK exit from the EU Implementation Period for up to date information on adequacy regulations and appropriate safeguards.

Related templates

For a 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/