

**Gloucestershire Local Medical Committee Guidance**  
**THE DATA PROTECTION ACT 1998 and**  
**THE FREEDOM OF INFORMATION ACT 2000**

*It is a while since these Acts came into force, but since they affect much of what we do, here is a reminder of how they affect practices.*

**The Data Protection Act 1998**

This Act came into force on 1 March 2000. It governs the release or otherwise of personal information. The Freedom Of Information Act (see below) governs all other information.

Under the 1998 Act living individuals are termed 'data subjects'. Under the Act a data subject has the legal right to:

- Obtain access to personal data of which he or she is the subject.  
Following a written request from a patient, GPs must:
  - Inform the patient whether personal data on that patient is being processed either by or on behalf of the GP; and
  - If information is held, the GP must give the patient a description of the personal data, the purposes for which it is being or will be processed and to whom that data is or may be disclosed.
- Apply for rectification or erasure of inaccurate data about the data subject.
- Seek compensation from the data controller for damage or distress caused by loss, destruction or unauthorised disclosure of either accurate data or inaccurate data in cases where the GP as data controller is unable to prove that he/she has taken such care as was reasonable in all circumstances to comply with the relevant requirement(s) of the 1998 Act
- Complain to the Data Protection Commissioner (DPC) when any part of the 1998 Act or separate provisions of the Act have been breached.

The 1998 Act clearly defines personal data to mean data that relates to a 'living individual' and does not apply to the records of deceased patients. (The health records of deceased patients are covered in England by the Access to Health Records Act 1990. (For guidance on access to the health records of deceased patients please see the BMA's 'Access to health records' guidance, June 2000)).

**The Eight Principles of the Data Protection Act 1998**

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 (see below) is met, and in cases of "sensitive personal data" (see definition below), at least one of the conditions in Schedule 3 (also below) is also met.
2. Personal data shall only be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes. If data that was collected previously is to be put to use for which consent was not originally granted then fresh consent needs to be obtained.
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed. Relevance of information is important here as it could be construed as a criminal offence to hold irrelevant information.

4. Personal data shall be accurate and, where necessary, kept up to date. *It is important to correct inaccuracies as soon as possible and note why the correction was made and when. Also any such corrected inaccuracy should be conveyed to a third party who may have been given the uncorrected original data.*

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. *Whilst the Act suggests that computerised records should not be kept once the person is no longer receiving services from the practice, from a medico-legal perspective this would not be acceptable. The DPC had agreed that until the electronic record and associated audit trail is reliably transferred the record should be made "inactive" or archived and not accessed unless for a valid reason. If an inactive record is accessed a record of why this access was made must be recorded.*

6. Personal data shall be processed in accordance with the rights of data subjects under this Act. *This simply requires you to comply with the "data subject's" access request except in such circumstances as defined in Sections 10, 11 & 12 of the Act.*

7. Appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. *This is self evident but it is important for someone in the practice to be appointed as being responsible for supervising data security procedures. This principle also embodies requirements in relation to staff involvement & information for patients; shredding of computer printouts; disposal of old computers, backup discs and tapes; backups, and, practice data and research.*

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

### **Schedule 2 of the 1998 Act - conditions for processing any personal data**

The most relevant conditions for GPs are as follows:

1. The data subject has given consent to the processing (NB: this does not have to be explicit consent, as for schedule 3)
2. The processing is necessary:
  - (i) for the performance of a contract to which the data subject is a party (it would appear that the data controller does not have to be a party as well); or
  - (ii) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject.
4. The processing is necessary in order to protect the vital interests of the data subject.

### **Sensitive Personal Data**

The 1998 Act defines sensitive personal data as the data subject's:

- racial or ethnic origin.
- political opinions
- religious beliefs or beliefs of a similar nature

- membership (or not) of a trade union
- physical or mental health or condition
- sexual history
- commission or alleged commission of any offence and any legal proceedings in connection with such an offence.

**Schedule 3 of the 1998 Act - conditions for processing “sensitive personal data”**

The conditions that must be satisfied before “sensitive personal data” can be fairly processed (including obtaining the data) are:

1. The data subject has given explicit consent to the processing of the personal data
2. The processing is necessary:
  - (i) In order to protect the vital interests of the data subject in cases where:
    - (a) Consent cannot be given by or on behalf of the data subject; or
    - (b) The data controller cannot be reasonably expected to obtain the consent of the data subject
  - (ii) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
  - (iii) for medical purposes and is undertaken by:
    - (a) a health professional; or
    - (b) a person who owes a duty of confidentiality that is equivalent to that which would arise if the person was a health professional.

The DPC considers that reliance on condition 2 (i) and (ii), stated above, may only be claimed when the processing is necessary for matters of life and death (e.g. the disclosure of a data subject’s medical history to a hospital casualty department treating a data subject after a serious road accident).

GPs need to be clear on the sort of data they are processing – is it personal data or “sensitive personal data”?

- When collecting personal data from an individual, e.g. name and address, (covered by schedule 2), GPs should ensure that individuals are not misled as to why it is required, what it will be used for and to whom it will be disclosed. This information could be passed on through personal contact at the time the data is collected, or via a notice displayed in the surgery waiting room, or in the practice leaflet. Patients should be given the opportunity to ‘opt-out’ of having their patient data used in any way other than those specified by themselves.
- However, all medical records fall within the definition of “sensitive personal data” and so the consent required under Schedule 3 must be explicit, i.e. the data subject would have to be given an opportunity actively and positively to signify their consent to the data processing. The DPC has suggested that using only practice leaflets to inform patients of the uses made of their “sensitive personal data”, may not sufficiently inform patients as to the degree of choice they have over the processing of their personal data.

The Act also requires that information obtained from a third party must be obtained in a way that is fair to the data subject. For example, the concept of

fairness requires that the data subject be informed when personal data about him/her has been obtained from a third party.

The collection and/or use of data for research (including historical and statistical purposes) needs special mention. There is provision in the 1998 Act that the processing of personal data for research purposes shall not be regarded as incompatible with the purposes for which the data was originally obtained. However, the fair processing requirement of the first principle may still require data controllers to inform individuals that their data may be processed for research purposes.

### **A Section 30 Exemption:**

Under powers given to him by Section 30 of the Act the Sec of State <sup>1</sup>, has exempted provisions relating to the data subjects' rights where access to the material about the patient's health and/or medical treatment may cause serious harm to the physical or mental health/condition of either the data subject or any other person.

## **The Freedom of Information Act 2000**

### **Introduction**

The Freedom of Information Act 2000 came into force on 1 January 2005. The Act requires that all public bodies (including GP practices) make available, with certain exceptions, information that is produced and held by them to members of the public if requested.

### **Requirements**

The Act requires that each public body shall produce by 1 Jan 2009, and thereafter shall maintain, a publication scheme. This is a document that details under seven broad classes:

- Who you are and what you do.
- What you spend and how you spend it (as regards public monies).
- What your priorities are and how you are doing it.
- How you make decisions.
- Your policies and procedures.
- Lists and registers.
- The services you offer.

The ICO has provided a template guide for general practitioners, which is available here:

[www.ico.gov.uk/Home/what\\_we\\_cover/freedom\\_of\\_information/publication\\_schemes/template\\_guides\\_to\\_information.aspx](http://www.ico.gov.uk/Home/what_we_cover/freedom_of_information/publication_schemes/template_guides_to_information.aspx)

### **Frequently Asked Questions**

***Who can request information?*** Under the Act, any individual, anywhere in the world, is able to make a request to a practice for information. An applicant is entitled to be informed in writing by the practice whether the practice holds information of the description specified in the request and, if that is the case, have the information communicated to him. An individual can request information, regardless of whether he/she is the subject of the information or affected by its use.

---

<sup>1</sup> [ Statutory Instrument 2000 No. 413 The Data Protection (Subject Access Modification) (Health) Order 2000]

### ***How should requests be made?***

Requests must:

- (i) Be made in writing (this can be electronically e.g. email/fax).
- (ii) State the name of the applicant and an address for correspondence.
- (iii) Describe the information requested.

**A practice must comply with a request within 20 working days.** Where a fee is required (see below), the deadline will be extended until the fee is paid.

If the practice transfers the request to another public authority, for example, the PCO, then the PCO also has 20 working days from receipt of the request to respond.

The applicant can request a copy of the information, ask to inspect the information or request a summary of the information. The Act requires practices to try and provide the information in the requested format. **A practice is not obliged to comply with repeated or vexatious requests for information. Therefore a practice can refuse to supply identical or substantially similar information to any one person if a reasonable time has not passed since the previous request.**

***If a member of the public requests information, but their request is unclear and the practice has to contact the applicant to clarify the information requested, does this affect the 20 day rule?***

Yes. If a practice subsequently has to contact an applicant to gain further information regarding the content of the request, then the 20 day response period is deemed to have started when the practice are quite clear of the information they are being asked to provide, not from the time of the original request. If the practice does not receive further information from the applicant, which is reasonably required, then the practice is not obliged to comply with the request.

### ***What is the process if practices do not want to disclose information?***

- Practices can only refuse to comply with the Act if one of the exemptions applies.
- GPs must issue a refusal notice to the person requesting the information. This refusal notice must deal with each request for information, stating clearly upon what grounds the GP is refusing to disclose.  
*NOTE: This is important because the Information Commissioner will rely on the grounds stated in the refusal notice when making a decision, if approached.*
- The refusal notice should state clearly what the appeals procedure is for a requestor, should he/she wish to contest the decision.
- Practices should have an internal appeals procedure in place as requestors will not be able to approach the Information Commissioner for a decision unless internal appeals procedures have been exhausted. This effectively gives both parties time to reconsider before the matter is elevated to the Information Commissioner.
- If referred to the Information Commissioner, the Information Commissioner will make a decision and inform the practice.
- If the Information Commissioner requires further information before making a decision, the practice will be issued with an information notice detailing what further information is required.
- If a practice fails to respond to a decision notice, an enforcement notice will be served and non-compliance could be regarded as contempt of

court, for which a judge may impose an unlimited fine or imprisonment. An appeals process is included in the Act.

***Are practices required to forward information to PCOs in order to fulfil requests made to the PCO under the Freedom of Information Act?***

On receiving a request for information any public authority must first ask whether or not it holds that information. If the authority has reason to believe that it does not hold the information, but that it is held by another public authority (e.g. the practice) then it is not obliged to obtain the information from the practice for the applicant. The PCO should forward contact details to the applicant for the relevant authority.

In some cases the authority may consider it appropriate to transfer the request to the relevant public authority. For further information please refer to Section 45, Part III, transferring requests, paragraph 19. If this is the case, then the receiving authority has another 20 working days from receipt to respond to the request.

***If we publish certain data annually, can we refer requests to this, rather than respond to the individual request?***

If the request matches the information already published, then the authority can refer the applicant to the material already published.

**The information – should it be disclosed or is it exempt?**

***Do I need to disclose information that is already available in the practice publication scheme or published elsewhere?***

The majority of the information requested should be covered in the practice publication scheme. Information which can be obtained elsewhere does not need to be disclosed. The practice can then refer the requestor to the appropriate website or publication scheme, for example information which is on the Department of Health website. Also if an individual makes a request for information that is included on the practice publication scheme, the request can be declined. Practices will therefore save themselves time by ensuring arrangements are in place to ensure that their publication schemes are up to date.

***What information can practices withhold?***

Some types of information are exempt from the requirement to make them available. These include:

- **Absolute** exemptions – this includes but is not limited to:
  - Personal information, the handling and disclosure of which is regulated by the Data Protection Act 1998.
- **Qualified** exemptions – this includes but is not limited to:
  - Information whose disclosure would harm the commercial interests of the public body or of a third party.

If a qualified exemption applies, the next step is to decide whether the disclosure satisfies the public interest test:

**The public interest test** - Information whose disclosure would harm the public good to an extent that is greater than the presumed public good of releasing it.

It generally appears that the public interest will outweigh non-disclosure where there is a question as to:

- (i) The transparency in the accountability of public funds.
- (ii) Whether there is proper scrutiny of government actions in accordance with published policy, and;

(iii) Whether public money is being used effectively.

However, only the exempt part of the document can be withheld. The rest of the document must be released when requested.

Any use of the exemptions under the Freedom of Information Act should be properly communicated to the applicant in a refusal notice. This should state whether the information is held and why it is believed to be exempt from disclosure under the Act.

It is important to note that in all instances where exemption is used and information is not disclosed, the applicant will be able to challenge this decision primarily through the complaints procedure of the public authority and then via the Information Commissioner.

If a practice needs time to consider whether a public interest test applies, then the 20 day rule is extended for a reasonable period.

### ***What is a vexatious or repeated request?***

The Freedom of Information Act also allows practices to refuse to fulfil a request for information in cases where it is deemed to be 'vexatious' or 'repeated'. It is necessary to apply this exemption fairly and consistently as practices may need to defend their decisions. The term 'vexatious' is not clearly defined in the Act, but the Information Commissioner has published guidance on the Information Commissioner website, and in Awareness Guidance No. 22, on which the following is based.

A request maybe vexatious if:

- The applicant makes clear his or her intention is for the purpose of annoying the practice in retaliation/annoyance then this would be grounds for refusal.
- The request does not have any serious purpose or value. If a patient was making a complaint about a doctor's treatment, and asked for information regarding similar complaints, this could be a valid request. If said patient sought information regarding every complaint levied at the practice, including other doctors, the cleanliness of the cloakroom etc, such information may be seen to have no serious purpose or value in relation to the initial complaint, and hence may be seen as vexatious.
- The request can fairly be characterised as obsessive or manifestly unreasonable. This is a very difficult category to define, but it is possible that practices will get repeat perpetrators of vexatious requests, and it is possible that the practice will have had continued contact with the applicant. This is not to say that the request is for the same information each time, (which could be refused as a repeated request), however, over a period of time a practice may decide that the number of requests from one person is designed to be a nuisance and so choose to refuse information for this reason.

These are by no means exhaustive.

### ***Who decides if a request is vexatious?***

It is to be decided within the practice whether or not a request is vexatious, however, the GPC would recommend that even when a competent staff member has decided that a request is most likely vexatious, it is advisable to refer the decision to a senior staff member/partner, given that the judgement may be contentious and have to be defended.

***We have been asked to provide information on the number of cases of mumps, measles and rubella, and also on the uptake of the MMR jab by a local newspaper. We only hold this information in individual records. We could find out this information, but are we required to extract it under the Act?***

If a practice holds raw data and receives a query for analysis it is not required to extract this information in order to provide it to the applicant. In the above scenario, the Data Protection Act would prevent all of the personal records from being disclosable. The time it would take to anonymise all of the records in order to provide the information in the format in which it is held would almost certainly take the cost over the appropriate limit, which means that the practice could refuse to provide this information.

***What is the difference between disclosures under the Data Protection Act and the Freedom of Information Act?***

Put simply, the Data Protection Act covers personal data, the Freedom of Information Act covers any other information held by the practice e.g. procedures, governance etc. On the whole, if an applicant asks to see personal data this would be exempt under the Freedom of Information Act. The applicant would need to submit a subject access request under the Data Protection Act. The Information Commissioner has advised that personal information can be released under the Act, in so far as the personal information is related to that person's role in the public authority and where disclosure does not breach any of the Data Protection Principles. An example would be NHS Salary pay bands. Further information can be found on the Information Commissioner's website at:

[www.informationcommissioner.gov.uk/cms/DocumentUploads/AG%2010%20Defence%20Exemp%20final.pdf](http://www.informationcommissioner.gov.uk/cms/DocumentUploads/AG%2010%20Defence%20Exemp%20final.pdf)

***Do individuals have a right to access information held about themselves under the Freedom of Information Act?***

If the applicant is requesting personal information **about themselves or another person** then there is **no right to know** under the Freedom of Information Act. However, such requests may become requests under the Data Protection Act and should be treated accordingly.

***Do internal emails need to be disclosed under FOIA?***

The Information Commissioner has advised that the Freedom of Information Act provides a general right of access to information held by Public Authorities, regardless of the form in which the information is held. Internal emails may therefore need to be disclosed under the Act. Do not forget that some of the information contained in the emails may be exempt, and other information may be supplementary to the boundaries of the request. Such information does not need to be disclosed.

Emails can be deleted during the normal course of business, however, emails must not be deleted with the intention of evading disclosure. It is good practice for practices to have a policy for the retention and disposal of documents, including emails. The GPC is expected to be issuing further guidance in this area.

***If a member of the public requests information regarding a work in progress, do we need to disclose this information e.g. draft documents/meeting notes if a decision is yet to be made?***

The Information Commissioner states that information must be disclosed regardless of the form in which it is held. Draft documents/meeting notes may therefore need to be disclosed unless otherwise subject to an absolute or

qualified exemption. Information intended for future publication is usually exempt.

***We are receiving requests for QOF data? Should we disclose this information or is it exempt?***

Under Section 22 of the Freedom of Information Act, data which is intended for publication would normally be exempt from disclosure. As a result, it is legitimate to refuse to disclose information on QOF before it is published. Once QOF data have been published, practices can refer enquirers to the appropriate websites.