

Data Protection Act 1998

The Data Protection Act has been in force and, hopefully, applied already by practices in the four years since its inception and the purpose of this short note is simply to remind members of the Eight Principles on which the Act is founded and, perhaps, to highlight a few points. This is based almost completely on GPC Guidance issued in September 2000 and updated in January 2004

"The Data Protection Act 1998 (**the 1998 Act**) came into force on 1 March 2000. The Act gives effect to the European Commission's Data Protection Directive 96/46/EC and replaces the Data Protection Act 1984 (**the 1984 Act**). Essentially, the 1998 Act regulates the way in which personal information about "living individuals" is processed and stored".

"Under the 1998 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:
 - (i) inform the patient whether personal data on that patient is being processed either by or on behalf of the GP; and
 - ii) 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.

This goes beyond the 1984 Act, which simply obliged GPs to supply the patient with a copy of any information constituting personal data on that patient.

(for further details about providing access to patient records and the fees GPs can charge please see the BMA's '*Access to health records*' guidance, June 2000)

- 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
- To complain to the DPC when any part of the 1998 Act or separate provision 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 by the Access to Health Records Act 1990 and Access to Health Records (Northern Ireland) Order 1993. (For guidance on access to the health records of deceased patients please see the BMA's '*Access to health records*' guidance, June 2000)".

NB. The 1998 Act covers all of the UK.

The Eight Principles

First principle

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 is met, and**
- **in cases of "sensitive personal data" (see definition below), at least one of the conditions in Schedule 3 is also met.**

Second principle

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.

Third principle

Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is processed.

Fourth principle

Personal data shall be accurate and, where necessary, kept up to date.

Fifth principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Sixth principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Seventh principle

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.

Eighth principle

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.

In the 1998 Act, "sensitive personal data" has been defined as the data subject's:

- o racial or ethnic origin
- o political opinions
- o religious beliefs or beliefs of a similar nature
- o membership (or not) of a trade union
- o physical or mental health or condition
- o sexual history
- o 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 [Data Protection Commissioner] 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 is disclosed. This information could be passed on through personal contact at the time the data is collected, 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 than 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 states 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.

Points to consider:

Second Principle: 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.

Third Principle: **Relevance** of information is important here as it could be construed as a criminal offence to hold irrelevant information,

Fourth Principle: It is important to correct inaccuracies as soon as possible and note why the correction was made and when. Also any such corrected inaccuracy conveyed to a third party who may have been given this.

Fifth Principle: Advice appears to be that 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.

Sixth Principle: This simply requires you to comply with the "data subjects" access request except in such circumstances as defined in Sections 10, 11 & 12 of the Act.

Seventh Principle: 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.

Eighth Principle: This is self-explanatory.

Section 30 Exemption: In secondary legislation, [*Statutory Instrument 2000 No. 413* **The Data Protection (Subject Access Modification) (Health) Order 2000**] the Sec of State 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. Further guidance was expected on this.

This is not an exhaustive synopsis of the DPA but covers principal points. For further more authoritative information it is suggested that you view the following websites:

www.bma.org.uk and search for Data Protection Act
www.dataprotection.gov.uk
www.legislation.hmsc.gov.uk/si/si2000/20000413.htm

Prepared on 5 January 2005 by
Dr Michael Uprichard
(from GPC "The Data Protection Act 1998: An updated code of Practice for GP's")