Advicesheet

Data Protection

B2

BDA advice

Advicesheet

Data Protection

B2

Dentists who process personal data about individuals must comply with the Data Protection 1998 (DPA).

This advice sheet describes the principles of the Act, the requirements it places on dental practitioners and gives practical guidance on compliance.

contents page

The Data Protection Act

The long title of the Act is: "An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information".

The Act, which applies to the United Kingdom, implements the EU Data Protection Directive (95/46/EC). The Directive protects an individual's right to privacy with respect to personal data.

The main provisions

Data users must

- notify the Office of the Information Commissioner if personal data is being processed automatically
- comply with the principles covering the quality of data
- obtain data fairly
- respect the right of access by the data subject and the right to correct inaccurate information processed automatically.

Data processed without reference to individuals is included (for example simple single-use mailing lists which are not kept up to date) and the Act applies to manual records as well as those processed automatically (except that processors of manual records do not need to notify). The conditions under which data can be processed are defined in law and special rules apply to 'sensitive' data, particularly the need to safeguard the rights and freedoms of individuals.

Definitions – personal data and records

'Data'

Data is information which:

1. *is being processed by means of equipment operating automatically in response to instructions given for that purpose, or*
2. *is recorded with the intention that it should be so processed, or*
3. *is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or*
4. *does not fall within the above but forms part of an accessible record.*

Manual health records are generally covered by the fourth category of data, that is, an accessible record.

'Personal data'

"*relates to a living individual who can be identified from those data, or from those data and other information in the possession of or likely to come into the possession of the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual.*"

'Accessible record'

The definition includes "*a health record (any record which (a) consists of information relating to the physical or mental health or condition of an individual, and (b) has been made by or on behalf of a health professional in connection with the care of that individual)*"

Clinical dental records are classed as accessible records for the purposes of the Act. Accessible records are subject to special provisions for subject access.

'Relevant filing system'

is "*any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible*."

What is a relevant filing system?

In order to decide whether manual information falls within a relevant filing system it is necessary to look at whether:

- there is a grouping together of information about individuals by reference to a distinct identifier that is under a common theme or element. These sets of information may not be in one file, one filing cabinet or one business premises and the identifiers might be in the form of codes, stickers or sub-sections within files
- the data is structured so that information is grouped either by name or personal identifier or by some criteria relating to the individuals, for example age, gender, occupation, type of treatment, payment method
- the filing system allows specific information about an individual to be readily accessible. There is no statutory definition of readily accessible, but current guidance is that the information must be capable of being reached easily by virtue of the way the file is structured. Dental records would generally be readily accessible.

So whether personal data comes within the scope of the Act depends on the way the information is grouped, structured and accessed, rather than the generic type of information. Information stored in a relevant filing system need not be in a file - card indexes, records of telephone calls or microfiche may all be covered depending on how the information is structured. The fact that information is contained in a file does not necessarily make it a relevant filing system. It is therefore difficult to give specific guidance on what types of manual information held within a practice will be covered but the following examples of personal data would come within the Act under normal practice circumstances:

- Patient record cards filed in a logical way (by name or number)
- A dentist's NHS schedule containing information about individual patients, their treatment and its cost
- A practice appointment book/day book containing readily accessible specific information about patients
- Lists of patients grouped according to the existence of bad debts, membership of private dental plans or other financial factors
- Patient records identified by stickers as having particular medical/dental conditions
- Patient address lists held on computer
- Identifiable radiographs and clinical photographs
- Letters about the patient from other health care providers
- Complaints records
- individual personnel files, as well as holiday and sickness records.

'Sensitive personal data'

means personal data concerning the data subject's

- racial or ethnic origin
- political opinions, membership of a trade union
- religious or other beliefs of a similar nature
- physical or mental health or condition, sexual life
- criminal offences, criminal proceedings and convictions.

Clinical dental records therefore come under the definition of sensitive personal data and special provisions apply to the processing of this data.

'Processing'

The definition of processing of data is very wide:

"*obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:*

- *organisation, adaptation or alteration, or*
- *retrieval, consultation or use, or*
- *disclosure by transmission, dissemination or otherwise making available, or*
- *alignment, combination, blocking, erasure or destruction.*

The Act requires that personal data is processed fairly and lawfully. Processing that is otherwise than by reference to the data subject is covered (for example a computer-held single-use-only mailing list.

It is very unlikely that a dentist would be processing personal data in a way that was not covered by the new legislation.

'Data subject'

is an individual who is the subject of personal data. In dental practice data subjects might be patients, practice employees or self employed contractors such as associates.

'Data controller'

is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

A data controller must be a legal entity, that is, an individual, a partnership, a company or organisation. Data controllers can act jointly or in common, that is they share decisions about the way personal data is processed or share a pool of personal data, each processing it independently of each other.

General practice arrangements

Single-handed practice owners, expense sharers (who are not partners) and associates are all data controllers, since they are responsible for their patients' clinical records and so determine the purposes for which the data are kept, as well as the manner in which the processing takes place (although for associates the way the practice is organised has a bearing on this). Whether expense sharers share a pool of patient data that they each process separately (and are therefore individual data controllers) depends on the specific arrangements that they have. For example, do the same staff members process the data in exactly the same way for all of the sharers? Are joint decisions made about processing? Dental partnerships in which the partners are jointly and severally liable and are one legal entity are treated as a single data controller.

Where there is a branch practice, only associate dentists who work only in that branch need to notify separately, since data controllers who work at more than one location are required just to list the addresses of the premises where data is processed.

Dentists employed as locums or assistants in general practice are not data controllers and are not responsible for complying with the Act. Dentists *employed* in the hospital and salaried primary dental care services and in corporate bodies will also not be classed as data controllers. It is likely that most of these dentists will have responsibility for abiding by the data protection principles contained in their contracts of employment.

'Data processor'

is *any person (other than an employee of the data controller) who processes the data on behalf of the data controller*.

A data processor is the same as a computer bureau under the DPA84. Practice owners and partnerships that engage associates will usually be acting as a data processor for them.

'Recipient'

in relation to personal data means *any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of the data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law*.

In dental practice a recipient could be, for example, a practice employee; private dental plan, PCT/BSA/Health Board employee; or a hospital consultant.

'Third party'

means any person other than:

- *the data subject*
- *the data controller*
- *any data processor or other person authorised to process data for the data controller or processor.*

For the purposes of this expression, employees or agents of the data controller or data processor are interpreted as being part of the data controller or data processor. A third party might be a police officer, judge or coroner.

Notifying the Information Commissioner (automated records)

Automated processing

Data controllers processing personal data by automated means are required to notify the Information Commissioner that they intend to process personal data. Automated processing includes computers, laptops, palmtops, notebooks and CCTV. The Commissioner holds a register of notifications that includes:

- The name, address, telephone, fax, e-mail and website (where appropriate) of the data controller
- The nature of the business of the data controller
- A description of the personal data and the data subjects
- A description of purposes and recipients
- Description of the measures that have been adopted to ensure the security of the data
- Safeguards for the transfer of personal data to non-EEA countries
- The date the entry was made in the register, date it was last amended and the date that it will be removed if the annual fee is not paid.

Notification must be purpose-based, purposes being chosen from a standard list. There are standard descriptions of data subjects, data recipients and third country transfers. The data controller must also give a brief description of the nature of the business, which is used by the Commissioner's Office to select the template notification form.

Processing of data cannot begin until the relevant date, that is the date the Commissioner receives the notification and fee or the day the Post Office received it if it was sent by recorded delivery or registered post. An annual fee is payable in order to retain a register entry. This fee is due twelve months after the relevant date and, if it is not received within fourteen months of the relevant date, the data controller will be removed from the register. It will be an offence to continue processing data whilst unregistered.

Data controllers who process data solely for the purposes of:

- pay and staff administration
- advertising, marketing and public relations
- keeping accounts, books and financial records
- the administration and membership activities of a non profit-making organisation

are exempt from the need to notify.

How to notify

To notify contact the Information Commissioner's Office either by telephone or the internet.

If you wish to begin the notification process by telephone, use the registration line below and the Office will record brief details about the data controller and the nature of the business. A draft notification form and guidance will then be sent out with some information already completed, depending on the type of business that has applied. The Commissioner's Office has a template for general dental practice.

The Information Commissioner's Office - UK

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Tel: 08456 30 60 60 or 01625 54 57 45
Fax: 01625 524510
E-mail: notification@ico.gsi.gov.uk
www.ico.gov.uk

Information Commissioner's Office - Scotland

28 Thistle Street, Edinburgh, EH2 1EN
Tel: 0131 225 6341
Fax: 0131 225 6989
Email: scotland@ico.gsi.gov.uk

Information Commissioner's Office - Wales

Cambrian Buildings, Mount Stuart Square, Cardiff, CF10 5FL
Tel: 029 2044 8044
Fax: 029 2044 8045
email: wales@ico.gsi.gov.uk

Information Commissioner's Office - Northern Ireland

51 Adelaide Street, Belfast, BT2 8FE, Northern Ireland
Tel: 028 9026 9380
Fax: 028 9026 9388
Email: ni@ico.gsi.gov.uk

Notification via the internet involves logging onto the Information Commissioner's website and completing a notification form online, printing it off and then sending it to the Commissioner's Office with the fee.

Completing the notification form (using the dental template) is reasonably straightforward. Part 2 includes a requirement for a security statement. Practices that have adopted the BDA model security information policy and have a practice confidentiality policy will be able to answer most of the security questions in the affirmative. BDA Practice Support can advise on completing the notification form and practice security measures.

Data controllers have a duty to keep their register entries up to date. Changes in the name or address, practice or intentions (in respect of data processing) must be notified promptly, no later than 28 days from the change event. Where a data controller is a legal partnership, changes in partners do not need to be notified separately. Changes to security measures must also be notified promptly and at the latest by the 28-day deadline. Changes involving new processing must be notified before the processing starts.

The annual fee for notification is £35 and the fee may be paid by cheque, direct debit or BACS. The Commissioner's Office will issue a reminder. It is a criminal offence to fail to notify where data processing is occurring unless an exemption applies.

Manual records

Data controllers holding manual records that are accessible or part of a relevant filing system are exempt from the need to notify. The exemption does not affect the need for data controllers to comply with other relevant parts of the Act, such as the right of subject access, the need for adequate security, the provision of information to data subjects and the adoption of confidentiality and data protection policies.

The data protection principles

Personal data shall be:

1. Processed fairly and lawfully
2. Obtained only for specified and lawful purposes and further processed only in a compatible manner
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Kept for no longer than necessary
6. Processed in accordance with the rights of data subjects
7. Kept secure
8. Transferred outside the EEA only if there is adequate protection.

The principles largely reflect ethical guidance for the management of dental records, but the first and seventh principles have specific implications for the way data are collected and stored.

Fair and lawful processing – the first principle

The first and most important data protection principle for dentists is that

"Personal data will be processed fairly and lawfully and, in particular, shall not be processed unless:

(a) at least one of the conditions in Schedule 2 to the Act is met, and
(b) in the case of sensitive personal data at least one of the conditions in Schedule 3 to the Act is also met".

Sensitive personal data includes health information.

It is essential to comply with these provisions in order to process data lawfully:

- Fair processing code
- Conditions for fair processing
- Consent to processing

Fair processing code

The Act gives specific guidance on the need to process data fairly, referred to by the Information Commissioner as the Fair Processing Code. We have incorporated the main parts of this code in our model data protection policy. Complying with the code does not of itself guarantee immunity from challenge but compliance will be treated as an indication of fair and lawful processing unless there is evidence to the contrary.

To comply with the code, it is essential that the person from whom the data is obtained is not deceived or misled as to the purpose or purposes for which it will be processed.

Data obtained from a person who is authorised or required by any enactment to supply it, will always be fairly obtained.

Conditions for fair processing

Before data is processed, a data controller is required to provide or make readily available to the data subject the following information:

- The name of the data controller
- The purpose or purposes for which the data is intended to be processed
- Any further information, given the specific circumstances in which the data is to be processed, that is necessary to ensure that processing of the data is fair.

For general practitioners this information should be provided as part of a data protection policy that is given to patients.

Compliance with the first principle depends on satisfying at least one of the conditions from Schedule 2 and at least one from Schedule 3 before processing personal data. Those in italics apply to personal data processed by health professionals.

Schedule 2 – all data

- Consent to processing by the data subject has been obtained (this must be positive not negative consent)
- Processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract
- Processing is necessary to comply with a legal (non-contractual) obligation
- Processing is necessary to protect the vital interests of the data subject (this must be a serious life or death matter)
- Processing is necessary to carry out certain public functions and for the administration of justice
- *Processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, unless the processing is unwarranted because it is prejudicial to the rights, freedoms or legitimate interests of the data subject.*

Schedule 3 – sensitive personal data

- The data subject gives explicit consent to the processing
- Processing is necessary to comply with an employer's legal duty
- Processing is necessary to protect the vital interests of the data subject or another person and consent cannot be given by the data subject or the data controller cannot reasonably be able to obtain it
- Processing is carried out for legitimate purposes by certain non-profit bodies (for example trade unions, political parties, religious organisations)
- The information has been made public by the data subject
- Processing is necessary in legal proceedings/obtaining legal advice
- The data controller is exercising legal rights
- Processing is necessary to carry out certain public functions and the administration of justice

- *Processing is necessary for medical purposes and is undertaken by a health professional or another individual who is bound by the same rules of confidentiality*
- Processing is necessary for equal opportunities monitoring
- As specified by *The Data Protection (Processing of Sensitive Personal Data) Order 1999*.

Processing data in general dental practice should only be done by the dentist in the course of pursuing legitimate interests as a provider of health care, which is one of the conditions of Schedule 2. Dental practice also falls into the "medical purposes" condition of Schedule 3, which covers both the management of health services and the care and treatment of patients. Provided that the data is processed in a way that maintains confidentiality and is not used for any other unrelated purposes (such as other commercial, political or social interests), then the data controller will be complying with the first principle of fair processing.

Consent to processing

In general, it is sufficient to provide information to patients about what and how data is processed in the practice. **In exceptional circumstances**, where processing is carried out for purposes **other than** the data controller's legitimate business and positive interests (or any of the above conditions), it will be necessary to obtain the explicit consent of the data subject to the processing of the personal data. Examples might be research interests.

Dentists are familiar with the principles of consent to treatment. Consent for data processing is different from consent for treatment in that obtaining consent can be partly or wholly delegated to members of the dental team.

Where data subjects are required to signify their consent to the processing of personal data, there must be direct communication between patient and practice. It is not sufficient to infer from a non-response to a letter or leaflet that consent has been obtained. Obtaining explicit consent will involve the patient:

- being given an explanation of how their personal data will be processed, together with a copy of the practice's Data Protection Policy
- being given the opportunity to ask questions
- signing a consent form and keeping it in their records.

Security and confidentiality – the seventh principle

The seventh principle states that

"*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*".

Dentists are required by the normal professional duty of confidentiality to ensure that personal data about patients is kept secure, which means preventing unauthorised access and disclosure and unauthorised destruction. In deciding whether existing measures are appropriate to satisfy this principle, the data controller should consider the following factors:

- The nature of the data
- Technological developments at the time in relation to security systems
- The cost of implementing any measures
- The reliability of staff who have access to the personal data
- The potential harm that might result from a breach of security.

Practice staff should be aware, *by means of a practice confidentiality policy*, of the importance of absolute confidentiality and instructed that under no circumstances should information be disclosed to anyone except under the direction of the patient's dentist. A model Practice Information Security Policy is included (below).

Unauthorised access

Access to personal health information should be on a "need-to-know" basis and staff contracts of employment should include a confidentiality clause. In order to prevent unauthorised access, it is advisable for access to computerised records to be dependent on passwords known only to essential staff and not easily discovered or implemented by chance. Staff responsible for maintaining computerised records must be fully trained to minimise the risk of error and the accidental loss of a record. Back-up copies should be stored in a secure and fire-protected place away from the computer installation, preferably off the premises. It is also essential that computer records have a full audit trail facility to prevent data being erased or overwritten and record details of any amendments made to the data including the date and by whom the data were amended. This is an essential medico-legal requirement.

Manual records should be stored in locked and fireproof cabinets and the practice premises should have adequate security facilities to help prevent entry by intruders. Data should not be left unattended (for example in the boots of cars).

Data controllers who undertake automated processing must also provide to the Information Commissioner, when notifying, information about security measures that have been adopted to comply with the principle, by means of answering some straightforward yes/no questions.

Personal health information warrants a high level of security because of the potential damage that could result to patients by unauthorised disclosure, but security measures need to reflect the size and administrative facilities of the dental practice. The BDA model data protection policy contains some suggested measures that balance these two factors.

As part of the notification process, data controllers must give information on the security measures at the practice, whether they have undertaken a security risk assessment and state whether they have an information security policy. Most practices will have undertaken a risk assessment as part of normal business and professional practice, for example looking at unauthorised entry to the premises, looking at where personal data might be seen by patients, personnel and unauthorised visitors to the premises. This assessment process will then lead to the implementation of policies and procedures that ensure information security. A model Practice Information Security Policy is included (below).

Associates

Data controllers also have express obligations where the data processing is carried out by a data processor. This will be the case in a practice with associates. The data processor (the practice) must provide sufficient guarantees of their security measures to the data controller (the associate). A contract must be in place between the data processor and data controller that provides that the data processor will only act under instructions from the data controller with regard to data processing and that the data processor will comply with the security obligations imposed by the seventh principle. A suitable clause in an associateship agreement would satisfy this requirement, for example:

As a processor of data for the associate, the practice owner will comply with the 1998 Data Protection Act. In accordance with the seventh data protection principle, the practice owner agrees that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data are data that relate to a living or dead individual who can be identified from those data and are data for which the associate is the data controller.

The practice owner agrees to act only on the instructions of the associate in the processing of the personal data.

Dental systems suppliers

The need for a written agreement also may apply to arrangements for maintenance or provision of a back up facility by a dental computer systems supplier. Dentists need to ensure that personal data will not be distributed to any unauthorised person or organisation, that it will remain accurate and not altered in any way and will be held securely. Data should also not be held by the supplier for any longer than necessary, so that once any maintenance work has been completed, any relevant data held should be deleted from the supplier's system.

We would therefore advise that in instances where systems suppliers are 'processing' personal data for dentists, the following paragraph be included in the contract between the parties:

As a processor of data for Dr [INSERT DENTIST'S NAME], *Dental Surgeon, [INSERT SUPPLIER'S NAME] dental system supplier will comply with the 1998 Data Protection Act. In accordance with the seventh data protection principle,* [INSERT SUPPLIER'S NAME] *agrees that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personal data shall also not be kept by* [INSERT SUPPLIER'S NAME] *dental system supplier for any longer than is necessary*.

Personal data are data that relate to a living or dead individual who can be identified from those data.

Furthermore [INSERT SUPPLIER'S NAME] *dental supplier agrees to act only on the instructions of Dr* [INSERT DENTIST'S NAME] *in the processing of the personal data*.

Relevant exemptions

There are three main exemptions to provisions in the Act that are relevant to dental practice.

Research purposes

Personal data may be processed for research purposes provided that the processing does not support decisions affecting particular individuals and is not done in such a way as to cause substantial damage or distress to the data subject. As long as the research is not published in a form that identifies the data subject, there is no right of subject access.

Health, education and social work

Data subjects generally have the right of access to their health records and there is an obligation on data controllers to inform individuals of the purposes for which their data will be processed. There is an exemption for health records where access or informing individuals about the purpose of processing might seriously damage their physical or mental health. A decision on whether or not to withhold access must always be taken by the dentist.

Disclosures required by law

Personal data may be disclosed where required by law, including a court order. Where necessary, disclosure may occur in connection with legal proceedings, for obtaining legal advice and to establish, exercise or defend legal rights. This provision enables dentists to pursue patients for non-payment of an account through the courts or defend a claim by a member of staff in an Employment Tribunal.

There are other exemptions relating to crime and taxation, regulatory activity, journalistic, artistic and literary purposes plus miscellaneous provisions, details of which are available on request from BDA Practice Support.

Individual rights and access to records

The rights of data subjects are now wider and encompass:

- Access to personal data (subject access)
- Preventing processing that is likely to cause damage or distress
- Preventing processing in direct marketing
- Automated decision-making
- Taking action for compensation from the data controller for damage following contravention of the act
- Rectification, erasure, blocking and destruction of inaccurate data
- Requesting the Information Commissioner to make an assessment of whether any part of the Act has been contravened.

Subject access

Data subjects have the right of access to their records. Patients often request access to their dental records, particularly radiographs. This section summarises the procedures for giving access to patients and further help is available from BDA Practice Support.

Requests for access

Who can obtain access?

Where the data subject who is making a request for access is a child (that is someone aged under 16), the data controller must make a judgement as to whether the child understands the nature of the request. If so, the data controller should reply to the child, but if not, the parent or guardian may make a request on the child's behalf and receive the reply. Parents or guardians should only make such requests in the child's interests, not their own. Where the child is capable of making a request for access, but a parent or guardian does so on his or her behalf, the data controller should be satisfied that the child has consented to the request for access.

Access should not be given to the parent or guardian where:

- the child has expressly indicated that it should not be disclosed
- the child has provided the information on the basis that it would not be disclosed
- the information has been obtained following examinations or investigation to which the child has consented in the expectation that such a disclosure would not occur.

Where a solicitor or other person makes a request for access on behalf of the data subject, the data controller should give access if satisfied that the data subject has consented to the disclosure. Normally the solicitor would supply a signed consent statement.

Where a patient is deceased, anyone having a claim arising from the patient's death may apply for access under the 1990 Access to Health Records Act (access is not allowed under the DPA98). When receiving such a request for access, the data controller must use judgement on what is relevant to the claim. Disclosure cannot take place without a court order where the patient has asked that a note be made on the records that they are not to be disclosed.

How should access be requested?

To obtain access, the data subject must make a request in writing (which may be delivered electronically, that is by fax or e-mail), pay the prescribed fee and provide any information that the data controller may reasonably require in order to be satisfied as to the identity of the individual and the location of the information.

Fees

In most circumstances a fee for access to computerised records may be charged up to a prescribed legal maximum of £10. This charge includes administration and photocopying costs. The fee is £50 for manual records.

What must be provided and when?

Within 40 days of the original request, or from the fee and/or identification information being provided, the data controller must supply the data subject with a permanent copy of the requested information unless the supply of a copy is not possible, copying would involve disproportionate effort or the data subject consents otherwise.

If more than one request has been made by the same individual within a reasonably short timescale and the data does not change frequently, the data controller may not have to accede to the request. The obligation will depend on the nature of the data, its purpose in processing and the frequency of the request in relation to the frequency with which the data changes.

The information must be supplied in an intelligible form and, where it is not intelligible, an explanation should be given. In dentistry it would be usual for the dentist to offer to provide an explanation of part or all of the record. The information supplied must be by reference to the information held on the day that the application was received, subject to any routine processing. Deletion of the data following a request is not permissible unless the deletion would have occurred anyway. This is not appropriate in dentistry.

Where a decision "significantly affecting" an individual is made solely by the processing of personal data by automated means, he or she must be informed when making an access request of the logic involved in that decision making. It is unlikely that this provision will be applicable to dentistry at the present time.

There is an exemption to the right of subject access if disclosure is likely to cause severe pain or distress to the data subject. BDA Practice Support is happy to provide further advice on this point.

Information about third parties

Where personal data about third parties is part of the record (including being identified as a source) it should be disclosed where:

1. the third party has consented; or
2. it is reasonable in all the circumstances to supply the information without consent; or
3. the information is contained in a health record and the other individual is a health professional who has compiled or contributed to the health record or has been involved in the care of the data subject in his capacity as a health professional.

In deciding what is reasonable in the circumstances in (2), the data controller should consider:

- any duty of confidentiality owed to the third party
- whether the third party has refused consent
- any steps taken by the data controller to obtain consent
- whether the individual is capable of giving consent.

The most common instance of information supplied by third parties in dentistry might be information contained in letters from hospital consultants about a patient's medical or dental condition or personal circumstances. This information should be disclosed to the patient on request except where it is likely to cause serious harm to the health professional's physical or mental health. This exemption is unlikely to be applicable in dentistry but BDA Practice Support will advise on individual circumstances. A health professional should be informed if his or her identity has been disclosed.

Preventing processing

The data subject may give the data controller notice in writing to cease or not begin processing personal data if such processing is causing or is likely to cause significant damage or distress to him/herself or another. The reasons must be specified and the data subject must establish that the damage or distress is unwarranted.

There are exemptions to this provision where the data subject has already consented to the processing; the processing is necessary for the entering into or performance of a contract to which the data subject is a party; the processing is necessary for the performance of a legal obligation; or the processing is necessary to protect the vital interests of the data subject.

Rectification

Where a record is inaccurate, a data subject can apply to a court to order the data controller to erase, amend, block or destroy the record. This is very unlikely to occur in dental practice and in these circumstances specific advice should be sought from BDA Practice Support.

Compensation

A data subject can seek compensation from a data controller for contravention of the Data Protection Act when damage or distress can be demonstrated. Examples in dentistry might be distress caused by breach of confidentiality, failure to obtain consent to processing, failing to keep data secure so that it is disclosed incorrectly, failing to retain clinical notes for as long as they are needed, or failing to provide subject access.

Direct marketing

The Telecommunications (Data Protection and Privacy) Regulations 1999 prohibit direct marketing by fax and by telephone to those who have objected to it.

The Act also gives individuals the clear right to prevent the communication, by whatever means, of any advertising or marketing material directed to them.

Further information on ethical marketing techniques for dentists is available in BDA Advice Sheet A6 *Marketing in Dentistry*.

Enforcement

Information/enforcement notices

The Information Commissioner is responsible for enforcement of the Data Protection Act. The Commissioner may be asked by a data subject to make an assessment of whether one or more data protection principles are being contravened by a data controller. The Commissioner has wide discretion in how the assessment is conducted. Where an assessment is being undertaken, the Commissioner may serve an *information notice* on the data controller requesting specific information about past or current processing in order for a view to be taken on whether or not the Act is, or has been, contravened. Data controllers may appeal against an information notice to a data protection tribunal. The Commissioner may also obtain a warrant to enter premises and seize information where there is reason to believe the Act is being contravened.

Where the Commissioner decides that there has been a contravention, an enforcement notice may require the data controller to comply with the Act. Failure to comply is a criminal offence except where the data controller successfully appeals and can demonstrate that all due diligence has been exercised in complying with the request.

Some examples of criminal offences are processing without notification (where this is required), failure to notify changes to a notification, unauthorised disclosure of information, unauthorised obtaining or procuring of personal data, failure to comply with a notice and enforced subject access (for example an employer requiring a prospective employee to supply a copy of his or her police/health records).

Members served with an information or enforcement notice advice should seek advice from BDA Practice Support or their defence organisation.

PRACTICE CONFIDENTIALITY POLICY

At this practice, the need for the strict confidentiality of personal information about patients is taken very seriously. This document sets out our policy for maintaining confidentiality and all members of the practice team must comply with these safeguards as part of their contract of employment/contract for services with the practice.

The importance of confidentiality

The relationship between dentist and patient is based on the understanding that any information revealed by the patient to the dentist will not be divulged without the patient's consent. Patients have the right to privacy and it is vital that they give the dentist full information on their state of health to ensure that treatment is carried out safely. The intensely personal nature of health information means that many patients would be reluctant to provide the dentist with information if they were not sure that it would not be passed on. If confidentiality is breached, the dentist/dental hygienist/dental therapist/dental nurse faces investigation by the General Dental Council and possible erasure from the Dentists or DCP Register; and may also face legal action by the patient for damages and, for dentists, prosecution for breach of the 1998 Data Protection Act.

General Dental Council

All staff must follow the General Dental Council's rules for maintaining patient confidentiality contained in *Standards for dental professionals and Principles of patient confidentiality*.

If confidentiality is breached, each registered dental professional involved is responsible to the Council for their individual conduct.

What is personal information?

In a dental context, personal information held by a dentist about a patient includes:

- the patient's name, current and previous addresses, bank account/credit card details, telephone number/e-mail address and other means of personal identification such as physical description
- information that the individual is or has been a patient of the practice or attended, cancelled or failed to attend an appointment on a certain day
- information concerning the patient's physical, mental or oral health or condition
- information about the treatment that is planned, is being or has been provided
- information about family members and personal circumstances supplied by the patient to others
- the amount that was paid for treatment, the amount owing or the fact that the patient is a debtor to the practice.

Principles of confidentiality

This practice has adopted the following three principles of confidentiality:

Personal information about a patient:

- is confidential in respect of that patient and to those providing the patient with health care
- should only be disclosed to those who would be unable to provide effective care and treatment without that information (*the need-to-know concept*) and
- such information should not be disclosed to third parties without the consent of the patient except in certain specific circumstances described in this policy.

Disclosures to third parties

There are certain restricted circumstances in which a dentist may decide to disclose information to a third party or may be required to disclose by law. *Responsibility for disclosure rests with the patient's dentist and under no circumstances can any other member of staff make a decision to disclose*. A brief summary of the circumstances is given below.

When disclosure is in the public interest

There are certain circumstances where the wider public interest outweighs the rights of the patient to confidentiality. This might include cases where disclosure would prevent a serious future risk to the public or assist in the prevention or prosecution of serious crime.

When disclosure can be made

There are circumstances when personal information can be disclosed:

- where expressly the patient has given consent to the disclosure
- where disclosure is necessary for the purpose of enabling someone else to provide health care to the patient and the patient has consented to this sharing of information
- where disclosure is required by statute or is ordered by a court of law
- where disclosure is necessary for a dentist to pursue a bona-fide legal claim against a patient, when disclosure to a solicitor, court or debt collecting agency may be necessary.

Disclosure of information necessary in order to provide care and for the functioning of the NHS

Information may need to be disclosed to third party organisations to ensure the provision of care and the proper functioning of the NHS. In practical terms this type of disclosure means:

- transmission of claims/information to payment authorities such as the DPD/SDPD/CSA
- in more limited circumstances, disclosure of information to the PCT/HB
- referral of the patient to another dentist or health care provider such as a hospital.

Data protection code of practice

The Practice's *Data protection code of practice* provides the required procedures to ensure that we comply with the 1998 Data Protection Act. It is a condition of engagement that everyone at the practice complies with the code of practice.

Access to records

Patients have the right of access to their health records held on paper or on computer. A request from a patient to see records or for a copy must be referred to the patient's dentist. The patient should be given the opportunity of coming into the practice to discuss the records and will then be given a photocopy. Care should be taken to ensure that the individual seeking access is the patient in question and where necessary the practice will seek information from the patient to confirm identity. The copy of the record must be supplied within forty days of payment of the fee and receipt of identifying information if this is requested.

Access may be obtained by making a request in writing and the payment of a fee for access of up to £10 (*for records held on computer*) or £50 (*for those held manually or for computer-held records with non-computer radiographs*). We will provide a copy of the record within 40 days of the request and fee (where payable) and an explanation of your record should you require it.

The fact that patients have the right of access to their records makes it essential that information is properly recorded. Records must be:

- contemporaneous and dated
- accurate and comprehensive
- signed by the dentist
- neat, legible and written in ink
- strictly necessary for the purpose
- not derogatory
- such that disclosure to the patient would be unproblematic.

Practical rules

The principles of confidentiality give rise to a number of practice rules that everyone in the practice must observe:

- records must be kept secure and in a location where it is not possible for other patients or individuals to read them
- identifiable information about patients should not be discussed with anyone outside of the practice including relatives or friends
- a school should not be given information about whether a child attended for an appointment on a particular day. It should be suggested that the child is asked to obtain the dentist's signature on his or her appointment card to signify attendance
- demonstrations of the practice's administrative/computer systems should not involve actual patient information
- when talking to a patient on the telephone or in person in a public area care should be taken that sensitive information is not overheard by other patients
- do not provide information about a patient's appointment record to a patient's employer
- messages about a patient's care should not be left with third parties or left on answering machines. A message to call the practice is all that can be left
- recall cards and other personal information must be sent in an envelope
- disclosure of appointment books, record cards or other information should not be made to police officers or Inland Revenue officials unless upon the instructions of the dentist
- patients should not be able to see information contained in appointment books, day sheets or computer screens
- discussions about patients should not take place in the practice's public areas.

Disciplinary action

If, after investigation, a member of staff is found to have breached patient confidentiality or this policy, he or she shall be liable to summary dismissal in accordance with the practice's disciplinary policy.

Employees are reminded that all personal data processed at the practice must by law remain confidential after your employment has terminated. It is an offence under section 55(1) of the Data Protection Act 1998, knowingly or recklessly, without the consent of the data controller [insert name], to obtain or disclose personal data. If the practice suspects that you have committed such an offence, it will contact the Office of the Information Commissioner and you may be prosecuted by the Commissioner or by or with the consent of the Director of Public Prosecutions.

Queries

Queries about confidentiality should be addressed to [contact name].

PRACTICE INFORMATION SECURITY POLICY

This Dental Practice is committed to ensuring the security of personal data held by the practice. This objective is achieved by every member of the practice team complying with this policy.

Confidentiality (see also the practice confidentiality policy)

- All staff employment contracts contain a confidentiality clause.
- Access to personal data is on a "need to know" basis only. Access to information is monitored and breaches of security will be dealt with swiftly by [insert contact name]
- We have procedures in place to ensure that personal data is regularly reviewed, updated and deleted in a confidential manner when no longer required. For example, we keep patient records for at least 11 years or until the patient is aged 25 – whichever is the longer.

Physical security measures

- Personal data is only taken away from the practice premises in exceptional circumstances and when authorised by [contact name]. If personal data is taken from the premises it must never be left unattended in a car or in a public place.
- Records are kept in a lockable fireproof cabinet, which is not easily accessible by patients and visitors to the practice.
- Efforts have been made to secure the practice against theft by, for example, the use of intruder alarms, lockable windows and doors.
- The practice has in place a business continuity plan in case of a disaster. This includes procedures set out for protecting and restoring personal data.

Information held on computer

- Appropriate software controls are used to protect computerised records, for example the use of passwords and encryption. Passwords are only known to those who require access to the information, are changed on a regular basis and are not written down or kept near or on the computer for others to see
- Daily and weekly back-ups of computerised data are taken and stored in a fireproof container, off-site. Back-ups are also tested at prescribed intervals to ensure that the information being stored is usable should it be needed
- Staff using practice computers will undertake computer training to avoid unintentional deletion or corruption of information
- Dental computer systems all have a full audit trail facility preventing the erasure or overwriting of data. The system records details of any amendments made to data, who made them and when
- Precautions are taken to avoid loss of data through the introduction of computer viruses

This statement has been issued to existing staff with access to personal data at the practice and will be given to new staff during induction. Should any staff have concerns about the security of personal data within the practice they should contact [insert contact name].

PRACTICE DATA PROTECTION CODE OF PRACTICE FOR PATIENTS

KEEPING YOUR RECORDS

This practice complies with the 1998 Data Protection Act and this policy describes our procedures for ensuring that personal information about patients is processed fairly and lawfully.

What personal data do we hold?

In order to provide you with a high standard of dental care and attention, we need to hold personal information about you. This personal data comprises:

- your past and current medical and dental condition; personal details such as your age, national insurance number/NHS number, address, telephone number and your general medical practitioner
- radiographs, clinical photographs and study models
- information about the treatment that we have provided or propose to provide and its cost
- notes of conversations/incidents that might occur for which a record needs to be kept
- records of consent to treatment
- any correspondence relating to you with other health care professionals, for example in the hospital or community services.

Why do we hold information about you?

We need to keep comprehensive and accurate personal data about our patients in order to provide them with safe and appropriate dental care. We also need to process personal data about you in order to provide care under NHS arrangements and to ensure the proper management and administration of the NHS.

How we process the data

We will process personal data that we hold about you in the following way:

Retaining information

We will retain your dental records while you are a practice patient and after you cease to be a patient, for at least eleven years or for children until age 25, whichever is the longer.

Security of information

Personal data about you is held in the practice's computer system and/or in a manual filing system. The information is not accessible to the public and only authorised members of staff have access to it. Our computer system has secure audit trails and we back up information routinely.

Disclosure of information

In order to provide proper and safe dental care, we may need to disclose personal information about you to:

- your general medical practitioner
- the hospital or community dental services
- other health professionals caring for you
- NHS payment authorities
- the Inland Revenue
- the Benefits Agency, where you are claiming exemption or remission from NHS charges
- private dental schemes of which you are a member.

Disclosure will take place on a 'need-to-know' basis, so that only those individuals/organisations who need to know in order to provide care to you and for the proper administration of Government (whose personnel are covered by strict confidentiality rules) will be given the information. Only that information that the recipient needs to know will be disclosed.

In very limited circumstances or when required by law or a court order, personal data may have to be disclosed to a third party not connected with your health care. In all other situations, disclosure that is not covered by this Code of Practice will only occur when we have your specific consent.

Where possible you will be informed of these requests for disclosure.

Access
You have the right of access to the data that we hold about you and to receive a copy. Access may be obtained by making a request in writing and the payment of a fee for access of up to £10 (*for records held on computer*) or £50 (*for those held manually or for computer-held records with non-computer radiographs*). We will provide a copy of the record within 40 days of receipt of the request and fee (where payable) and an explanation of your record should you require it.

[*Note: this paragraph should be edited to relate to the circumstances of the practice. Some practices prefer not to make a charge*]

If you do not agree

If you do not wish personal data that we hold about you to be disclosed or used in the way that is described in this Code of Practice, please discuss the matter with your dentist. You have the right to object, but this may affect our ability to provide you with dental care.

Checklist

To comply with the 1998 Data Protection Act a practice must:

- have in place a data protection policy, a confidentiality policy and an information security policy
- have adequate security measures to ensure that there is no unauthorised access to data by third parties and data will not be destroyed by accident
- give patients access to their records and, where a charge is made for access or for copies, observe the statutory maximum
- where data is processed automatically, notify the fact every year to the Information Commissioner and pay the fee . Every dentist who has legal responsibility for patients whose personal data is processed automatically must notify separately (except for dentists in partnership)
- advise new and existing patients that the practice will be processing their personal data and be given a copy of the practice's data protection code of practice
- where a practice owner is providing data processing services to an associate, have a written agreement (a suitable clause in an associateship agreement) covering security and an undertaking by the practice owner to process the data in accordance with the associate's instructions
- where a dental systems supplier is processing data on behalf of a dentist, have a contract in place ensuring that the supplier complies with the Act and processes the data in accordance with the dentist's instructions.

BDA advice

British Dental Association
64 Wimpole Street London W1G 8YS Tel: 020 7563 4563 Fax: 020 7487 5232
E-mail: enquiries@bda.org www.bda.org