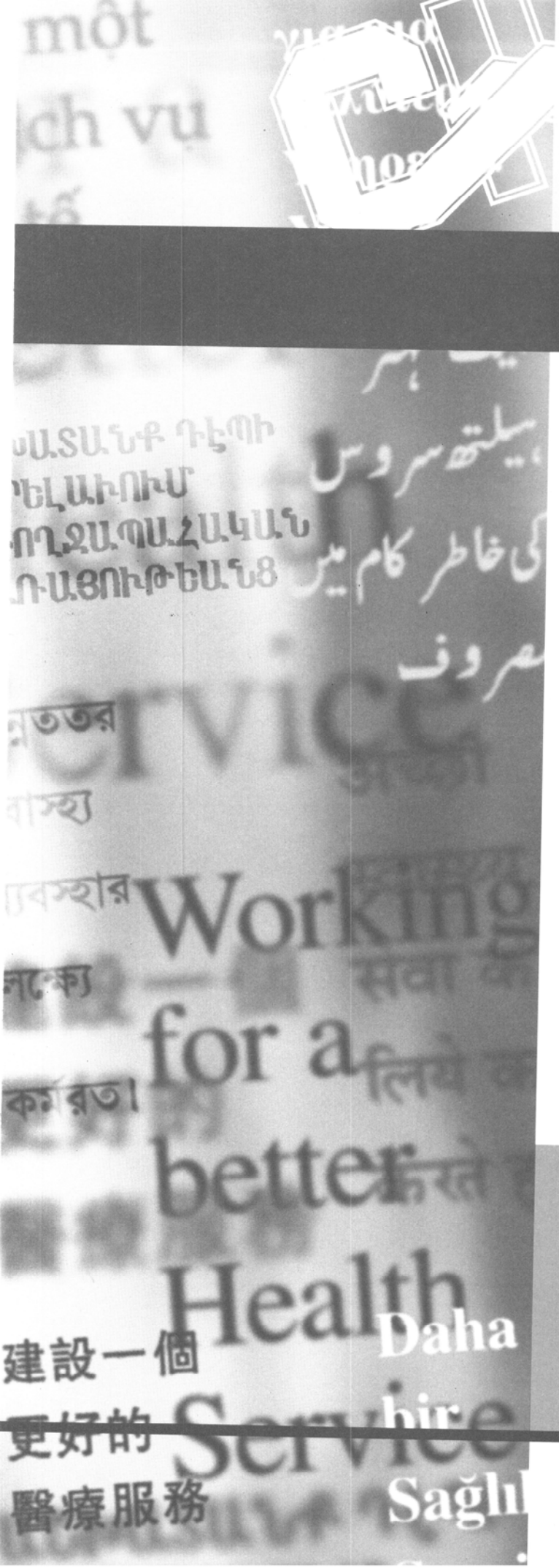

A QUESTION OF CONFIDENCE?

A guide to the Data Protection Act 1998

Marion Chester

June 2002

An examination of the balance struck between privacy and openness in the legal regime governing the use of information in the NHS. The provisions of the DPA are explored and their strengths and weaknesses are assessed and compared to provisions under the common law and Article 8 of the European Convention on Human Rights. Advice is also provided on using the Act to access information and enforcing it where it has been breached.

ASSOCIATION OF
COMMUNITY HEALTH COUNCILS
FOR ENGLAND & WALES

CONTENTS

INTRODUCTION 1

BACKGROUND 2

- Reason for Data Protection Legislation 2
- New UK Legislation 2
- New Terms 2

THE LEGAL FRAMEWORK 3

- The European Convention on Human Rights (ECHR) 3
- The EU Data Protection Directive 95/46 3
- Common law 3
- The Data Protection Act 1998 3
- Hierarchy of Laws 3

HEALTH RECORDS 4

- Health Professional 4
- Data Controller 5
- Additional Exemptions and Provisions 5

RIGHTS OF ACCESS TO INFORMATION 5

- Accessible Records 5
- The Process 5
- Access to Original Records 6
- Right to an Explanation 6
- Exemptions from the Duty to Provide Subject Access 6
- Accessing other people's records 7
- Charges for Access to and Copies of Records 8
- Accuracy 9

CONFIDENTIALITY 9

- Statutory Law 10
- The Common Law 11
- Article 8 of the European Convention on Human Rights 14

FAIR PROCESSING 16

- Duty to Notify Data Subjects of the Existence of Records 16
- Preventing the Use of Information 16

ENFORCING DATA PROTECTION RIGHTS 17

WHAT THE DATA PROTECTION ACT DOES NOT COVER 18

- Records of the Deceased 18
- Anonymised Information 18
- Medical Reports for Insurance and Employment Purposes 19

CHCS - COMPLIANCE WITH THE DATA PROTECTION ACT 19

APPENDIX 1 - THE DATA PROTECTION PRINCIPLES 20

FURTHER READING 21

BIBLIOGRAPHY 21

INTRODUCTION

Patients need to be able to access their own medical records in order to be able to participate in and feel confident about decisions relating to their health care. The protection of records from unauthorised disclosure is necessary to ensure that patients feel secure when divulging intimate personal information that clinicians may require for the purposes of providing effective diagnosis, treatment and care. The data protection regime is supposed to provide rights of access to patients' own records and safeguards against unauthorised uses and disclosures.

The NHS is subject to many pressures. Some of these conflict. Patients expect that relevant information from their records will be available to all treating clinicians. Lost and mislaid files or inaccurate information on them can compromise their care. Demands for access to patient information by those planning and monitoring services and by the medical research establishment run counter to patient expectations that their records will only be shared with health service staff engaged in their care. Clinicians do not expect the health service to require them to operate in ways that breach guidance issued by their regulatory bodies. A system of legal regulation of patient data is needed to ensure that these needs are balanced and that where conflicts arise, they can be resolved.

As electronic patient records become more widely used and more innovations are introduced utilising advances in information technology, it has become more important that patients are able to access their own records and to know who else may be accessing them. Legal mechanisms, which were once sufficient to protect patient records held in paper form, need to be regularly updated.

This area of law and the policies underpinning it are continuously under review. The Government are currently considering new initiatives for sharing personal data between government departments.[1]

This briefing details the legal system currently in place to regulate the use of patient information, assesses how well it lives up to the expectations and requirements of patients and considers whether it operates as an effective check on the NHS.

[1] *Privacy and Data Sharing. The Way Forward for Public Services.* Cabinet Office Report.

BACKGROUND

The Data Protection Act 1998 (referred to in this briefing as 'the DPA' or 'the Act') came into force on 1st March 2000. Later that year the Human Rights Act 1998 was brought into force and freedom of information legislation[2] was passed. The latter has yet to be brought into force. In order to understand the effect of UK data protection legislation on patient rights the impact of these three statutes on each other and on other legislation, must be considered together with the common law.

Reason for Data Protection Legislation

The DPA was introduced to ensure that the UK complies with the provisions of EU Directive 95/46. This European Directive (the Privacy Directive) was developed in response to perceived threats to individual citizens' autonomy over the confidentiality of their records, posed by data processing systems operated by governments and private concerns. Lord Hoffman succinctly expressed this concern when he said *'The right to keep oneself to oneself, to tell other people that certain things are none of their business is under technological threat.'*[3] The Directive also seeks to facilitate the free movement of information across member states within the European Community.

New UK Legislation

The 1998 Data Protection Act replaces and expands on the provisions of the Data Protection Act 1984, repeals the Access to Personal Files Act 1987 and substantially repeals the Access to Health Records Act 1990. The resulting changes impact on patients in two particular respects. Patients have changed rights of access to their health records. Data protection principles govern the use of personal information and as such are supposed to protect the confidentiality of patient records.

The DPA applies to most records that contain identifiable personal data, whether they are stored in computerised form or manually.

The Act places a number of welcome new requirements on the holders of records that contain information of a personal nature. Data controllers have a duty to advise people that they hold personal information about them and to advise of the source of information. However, these requirements are subject to a number of exemptions and are paid little more than lip service by the NHS.

New Terms

The Act contains a number of new terms. Records are referred to as 'personal data', record holders are called 'data controllers', and the individuals whose personal information is being held are called 'data subjects'. The Act concerns the processing of data, which is defined to include almost anything that can be done to recorded information including gathering, organising and disclosing or just keeping it. In this briefing these terms are used together with more easily understandable terms. In general, I refer to individuals or patients instead of data subjects, medical records instead of personal data and data controllers are variously referred to as record holders, clinicians, doctors, health bodies, hospitals, etc depending on the situation being examined.

The Data Protection Registrar has become the Information Commissioner and has powers to consider complaints by individuals who consider that their rights have been infringed. She has also been given powers to ensure that the law is complied with.

[2] Freedom of Information Act 2000
[3] R v Brown [1996]

THE LEGAL FRAMEWORK

An individual's right to control the use to which their personal information is put is protected by the UK common law, the application of Article 8 of the European Convention on Human Rights (ECHR), the EU Data Protection Directive and, to a lesser extent, by UK data protection legislation.

The European Convention on Human Rights (ECHR)

The most fundamental of these legal protections is to be found in Article 8 of the ECHR. This Convention was incorporated into UK law by the enactment of the Human Rights Act 1998. All public bodies and courts in the UK have to comply with and protect the human rights detailed in it as does any person or body carrying out functions of a public nature. UK legislation has to be interpreted in such a way that it is compatible with the Convention.

Article 8 is the provision relevant to those handling personal information. It states:

'Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right, except such as in accordance with the law and is necessary in a democratic society, in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

Cases brought under this article in the European Court of Human Rights have confirmed that it encompasses the right to see personal files and to have personal information kept in confidence. However, these rights are not absolute and public bodies are permitted some incursions into the private lives of citizens if to do so is justifiable in the public interest. In the case of medical records, disclosures not sanctioned by patients may be permissible if domestic law provides for it, and if it is necessary for the protection of health and is proportionate to the objective sought.

The EU Data Protection Directive 95/46

The Directive is based upon the Article 8 framework and lays down a number of principles to be applied by every EU government. It requires each member country to implement domestic legislation to provide rights of access to data subjects and to place a duty of confidentiality on those processing personal data, subject to the public interest override detailed above.

Common law

In the UK the courts have long recognised the right to confidentiality, although not a right of access to personal or health records[4]. The latter right was only introduced in the UK by legislation in the 1980s and 1990s. However the absence of a common law right of access to personal records does not preclude record holders voluntarily acceding to a request. The European Court of Human Rights has held that Article 8 of the Convention gives a qualified right to access personal records[5]. The introduction of the Human Rights Act 1998 is having an impact on the approach taken by the courts to applications of this nature[6].

The Data Protection Act 1998

This is the UK enaction of the requirements contained within the Privacy Directive; together with a raft of secondary legislation, it governs living patients' rights of access to their records and provides a privacy framework within which the NHS is supposed to operate.

Hierarchy of Laws

The interaction of these legislative regimes is fairly complex. The provisions of Article 8 take priority, but are interpreted in

[4] R v Mid-Glamorgan Family Health Service Authority ex parte Martin [1995]
[5] Gaskin v UK [1989]
[6] R on the application of Ann Stevens and Plymouth City Council and 'C' [2002]

accordance with each EU country's legislative and public interest requirements. This complicated interaction of laws is particularly illustrated by the position regarding the protection of patient confidentiality. UK data protection legislation was and continues to be drafted with an eye to permitting the state to make use of patient records for a wide range of purposes.

Data Protection Principle One as detailed in the Data Protection Act 1998, provides

'Personal data shall be processed fairly and lawfully...'

Lawfully refers to the requirements imposed by Article 8 and the common law. The DPA and secondary legislation supplementing its provisions go on to detail a large number of circumstances in which disclosure without consent is to be deemed lawful. If disclosures permitted by the legislation are challenged the courts will have to consider whether the legislation complies with Article 8. Those parts of regulations and orders which do not comply can be struck out. If a court considers that the Data Protection Act itself is at fault, then it can make a 'declaration of incompatibility' and ask Parliament to look again at the Act.

There are some gaps in the Data Protection Act 1998. It does not fully enact the Privacy Directive. Where such discrepancies come before the courts, then the court will apply the Act as if it did actually contain the relevant provisions of the Directive.

HEALTH RECORDS

The DPA governs the use of personal records held in many forms. Some of its provisions are specific to health records, which are defined in section 68 as follows:

'(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.'

Health Professional

Section 69 details who is a health professional for these purposes and therefore limits what is a health record, to those records made by:

- A registered medical practitioner.
- A registered dentist as defined by section 53(1) of the Dentists Act 1984.
- A registered optician as defined by section 36(1) of the Opticians Act 1989.
- A registered pharmaceutical chemist as defined by section 24(1) of the Pharmacy Act 1954 or a registered person as defined by Article 2(2) of the Pharmacy (Northern Ireland) Order 1976.
- A registered nurse, midwife or health visitor.
- A registered osteopath as defined by section 41 of the Osteopaths Act 1993.
- A registered chiropractor as defined by section 43 of the Chiropractors Act 1994.
- Any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 for the time being extends.
- A clinical psychologist, child psychotherapist or speech therapist.
- A music therapist employed by a health service body.

- A scientist employed by such a body as head of a department.

Data Controller

For the purposes of the DPA, the individual clinician may be the data controller, but if they work for a health service body, who retains control of records, that health service body will be the data controller. In general, primary care records are held by the relevant clinician. Hospital records are held by the NHS trust concerned. In practice is has not proved difficult to identify the data controller holding patient records.

Additional Exemptions and Provisions

There are a number of additional provisions in the data protection legislation, which mean that health records are treated somewhat differently to some other records. The same rights of access apply as to other records, but there is an additional exemption where disclosure would cause serious harm – see page 7. Higher charges can be levied for the supply of copies than is the case with other sorts of records - see page 10. Additional conditions apply before processing, including disclosure, can be carried out - see page 12.

To further complicate matters, different transitional arrangements apply to the processing of manual health records to those applicable to the processing of automated (computerised) records, most particularly in relation to the application of data protection principles; 1 (confidentiality), 2 (processing only for purpose obtained), 3 (information not excessive) and 4 (accuracy). Thus until the end of the second transitional period in October 2007, some of the protections afforded to automated health records are not fully available to patients whose records are held in paper form.

However it is important to bear in mind that the Act applies to all personal records whether or not they comprise health records.

RIGHTS OF ACCESS TO INFORMATION

Section 7(1) of the DPA provides a right of access to the data subject to *'information constituting any personal data of which that individual is the data subject'*. Section 8 (2) provides a right to be supplied with a copy of the same.

Accessible Records

Patients have the right to see their own records whether they are stored in computerised form, are hand-written or stored in some other form. The courts and the Information Commissioner have confirmed that rights of access extend to X-rays, scans, reports, and other material held on patients.

Under the previous legislative regime, access to medical records was restricted only to those records made after November 1991. However, this cut off date no longer applies and patients have the right to see all their old records, so long as they are still in existence.

Rights of access apply to other personal data kept by health bodies, including complaints records.

The Process

Although some record holders are happy to provide access following a verbal request, receipt of a written application by the data controller triggers the legal rights under the Act. The applicant does not have to give a reason for wishing to see the record. Sufficient information should be provided in the application to allow the data controller to be able to identify the data subject and their record. Name and address and date of birth should usually suffice. The application should be accompanied by the prescribed fee – see page10.

The data controller is required to comply with the request within 40 days unless they no longer hold the record, or information from the record cannot be disclosed for any of the reasons detailed below.

Access to Original Records

Section 7(1) of the Act does not appear to give data subjects the right to access original records, but only *'information constituting any personal data'*. While this will usually not cause a problem, it may do where there are allegations that records have been tampered with or are inaccurate and where only access to the original record will be sufficient to resolve a question or dispute. In this situation it may be necessary to obtain a court order requiring the production of original records.

Right to an Explanation

Section 7(1)(c) of the Act requires data controllers to communicate information from records and about their source in an intelligible form. This reproduces the previous requirement[7] that record holders must provide an explanation of unintelligible records, whether these are unintelligible because they are illegible or for some other reason, such as the use of technical terms. No charge can be made for the supply of such an explanation.

Exemptions from the Duty to Provide Subject Access

There are a range of exemptions to the duty to provide access. However, in practice they are rarely invoked. The Information Commissioner has made it known that her office will take action against data controllers who attempt to misuse the legislative provisions containing the exemptions.

Serious Harm

Secondary legislation in the form of The Data Protection (Subject Access Modification) (Health) Order S.I. 413 2000 provides that access can be refused, if in the opinion of the record holder (having taken advice from an appropriate medical professional), disclosure would cause serious harm to the patient's physical or mental health or condition or that of another person. Simple embarrassment is not a sufficient reason for withholding the record. The same order places a duty on record holders who are not health professionals to ensure that they consult an appropriate health professional to establish that such serious harm would not be caused by disclosure, before releasing information from medical records that they hold. The test to be applied is not whether it is in the patient's best interest to see the records, but whether serious harm will be caused by disclosure. Where serious harm would be caused by disclosure of part of the record, the remainder must still be disclosed.

Disclosure of Personal Information about Others

The duty of confidentiality means that records containing personal information about an individual should not be revealed without the consent of that person. Section 7(4) of the DPA confirms that if a record holder cannot comply with a request for access without disclosing information about a third party, the request can be refused unless either the individual concerned consents to the disclosure or it is reasonable to disclose without their consent. However this does not apply if;

(a) the third party is a health professional who has compiled or contributed to the record or been involved in the care of the patient[8], or

(b) the reference to the third party is limited to a reference that that person was the source of information on the record and the information can be made available minus the name of the source[9],

in either of these cases the consent of the third party is not required.

Disproportionate Effort

The statutory rights of access that are contained within the Act are subject to an exemption where the supply of the information would *'involve disproportionate effort'* – section 8(2)(a). Disproportionate effort is not defined in the Act. Many NHS trusts, health authorities and GPs complain that the supply of this information involves the use of scarce resources, which could be put to better use. The office of the

[7] Section 3(3) Access to Health Records Act 1990

[8] The Data Protection (Subject Access Modification) (Health) Order S.I. 413 2000

[8] Section 7(5) Data Protection Act 1998

information Commissioner indicated that they would take firm action if holders of health records sought to abuse this exemption. In practice, it does not appear that this exemption is often claimed as a reason for refusing access or copies of medical records.

Information Available under other Enactments

Any records, which could be accessed under open government legislation, are also exempt from the subject access provisions – section 34 DPA.

Other Exemptions

Other exemptions to the duty to provide access include:

- Once a request has been complied with, subsequent similar or repeat applications can be refused – section 8(3) DPA.

- Information held for research purposes – section 33 DPA. This exemption is subject to three safeguards. These are that;

1. data subjects cannot be identified from the results of the research,
2. the processing of the data does not cause substantial damage or distress to the data subject and
3. the data used in the research is not then used to make decisions about individuals.

- Where the provision of information would interfere with regulatory activities designed to protect members of the public or carried out for health and safety at work reasons – section 31 DPA.

- Registers kept by the Human Fertilisation and Embryology Authority – The Data Protection (Miscellaneous Subject Access Exemptions) Order S.I. 2000 419. Access rights are instead provided for at section 31 of the Human Fertilisation and Embryology Act 1990.

- Records held for tax purposes or for the prevention or detection of crimes including those involving misuse of public monies – sections 29 and 31 DPA.

- Where national security would be compromised – section 28 DPA.

- Where the provision of information would have an inevitable prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy – The Data Protection (Corporate Finance Exemption) Order 2000 S.I. 184.

Accessing other people's records

There is no express provision in the DPA for applications for access to be made on behalf of others. Before the Act came into force ACHCEW expressed concern about these omissions. In response, the Home Office and Department of Health insisted that the rights of children, those without the mental capacity to make an application on their own behalf and those acting through agents would be protected through the application of the common law. Although the common law principle of agency enables adults with capacity to authorise another person to make an application on their behalf, those without the mental capacity to make such a request do not have the capacity to instruct another person to do so either.

Agents and Representatives

Patients can ask the record holder to make the record or part of it available to another person, for example to their legal representative or a person assisting them with a complaint. Written authorisation is preferable. If a third party is authorised by the patient to make the application for access, the data controller is obliged to comply with it as if the application had been made by the patient. No additional charges can be levied.

Incapacitated Adults

Carers of adults without mental capacity have, in some instances, experienced difficulties in persuading holders of medical and personal records to disclose them. The DPA does not provide an explicit right for family members or carers to see the records of those without the mental capacity to ask for them themselves. Curiously secondary legislation expressly details the circumstances in which information is not to

be supplied to parents or to those seeking access on behalf of a mentally incapacitated adult[10].

The common law does not provide a right of access to records of adults who are deemed to be mentally incapable of giving authorisation for disclosure, but does provide protection for their confidentiality This duty of confidence is often cited by those resisting disclosure. Previously, the Access to Medical Records Act 1990 provided that another person could make application for access in these circumstances so long as they were doing so in their capacity as the person appointed by a court to manage the affairs of the incapacitated person. This was not ideal, and caused problems in many cases where the Court of Protection had not appointed a Receiver, or where the record holder did not recognise the legitimacy of requests made by carers and family members seeking to pursue the data subject's interests. In the case of Stevens v Plymouth City Council [2002] the local authority decided that the next relative (a position recognised in statute where a guardianship order is made) of a mentally incapacitated adult should not be given access to social services files.

Those denied access to medical records of incapacitated adults that they care for, can still apply to the courts for an order for disclosure. In this case the Court of Appeal stated that the Data Protection Act was of little assistance. Instead the court decided that having balanced the rights of confidentiality against the right to family life contained in Article 8 of the ECHR, disclosure to the patient's mother was justified.

Children

Parents can still apply to see their children's records although health professionals will still have to consider whether granting access to the parent is in the child's best interest. The Data Protection (Subject Access Modifications) Order S.I. 2000 No. 413 provides that information will not be supplied if the child has either expressly stated or has indicated in some other way that they wish it to be kept confidential. (The same provisions apply to applications for access to information held on a mentally incapacitated adult.) Older children with 'sufficient understanding and intelligence to understand fully what is proposed' can apply for access to their own records, or authorise their parents to do so on their behalf.

Charges for Access to and Copies of Records

At section 7(2) of the Data Protection Act 1998 provision is made for a fee to be charged for access to personal records. Charges can be made both for access and the provision of copies.

One of the main deterrents to patients wishing to access their own medical records are the charges which record holders in the NHS can make for access to and copies of these records. One effect of charges is that complainants are disadvantaged and are unable to pursue their complaints effectively. Some complainants find that they are the only people at an independent review hearing without a copy of their records in front of them. The EU Privacy Directive requires Member States to guarantee the right to obtain information without excessive delay or expense.

Secondary legislation[11] provides as follows:

- The maximum fee which can be charged to provide access is £10 except where a manual record has been added to or altered within a 40 day period prior to the application, in which case no fee is payable for access.

- A fee of up to £50 can be made for the provision of copies of medical records. This includes the £10 access fee where applicable. This charge applies even if the record has been added to within the previous 40 days.

The Information Commissioner and the courts have confirmed that the record includes x-rays and scans and that even if copies of these are sought the data

[10] The Data Protection (Subject Access Modification) Health) Order SI 2000 No 413

[11] The Data Protection (Subject Access)(Fees and Miscellaneous Provisions) Regulations S.I. 2000 No.191

controller cannot charge more than the £50 maximum.

Accuracy

Rights to have corrections made to records are provided for in the DPA. The fourth data protection principle detailed in Schedule 1 of the 1998 Act requires that information held should be accurate, but there is no express requirement that omissions be remedied. Section 70(2) of the Act provides. *'For the purposes of this Act data are inaccurate if they are incorrect or misleading as to any matter of fact.'*

In fact, there are currently two regimes governing accuracy. Patients with concerns about the accuracy of automated health records have rights under section 14 of the Act. Those whose records are still held in paper form have slightly different rights under section 12A of the Act[12].

If patients consider that information in their records is not accurate or is incomplete and the health professional refuses to make the necessary correction a complaint can be made to the office of the Information Commissioner who may rule that any erroneous information is rectified, blocked, erased or destroyed. In the case of automated records, section 14 of the Act provides a right to apply to a court for an order that inaccurate data be rectified, blocked, erased or destroyed or for a note to be placed on the file detailing the true facts. Section 12A makes similar provisions for the correction by a court of inaccuracies in manual records.

CONFIDENTIALITY

Patients provide sensitive information about themselves to GPs and other medical practitioners in the NHS. Believing this information will be treated in confidence they reveal marital problems, sexual histories, mental health concerns and a range of other information including information about other family members and possible genetic pre-dispositions to medical conditions.

Doctors have an interest in receiving this information, so that they will be able to accurately diagnose and treat problems. For as long as there has been a medical profession, the notion that these confidences must be respected has been a central tenet. Doctors know that breaches of confidence have the potential to destroy patient trust with the result that patients may in future withhold possibly vital information. A widespread breakdown of patient trust would have serious consequences not only for the treatment of individuals but for public health.

Patients recognise and accept that information they divulge may be passed onto other medical practitioners who will be engaged in their treatment. However, the NHS now requires medical practitioners to pass on identifiable patient information for a variety of other purposes, including financial and clinical audit and planning of health services. Once information has been passed on it may be used for a multitude of other purposes, including research carried out both within the NHS and in the private sector.

In the past, the physical nature of patients' notes provided some protection. GPs were much more easily able to control who had access to them. The growing use of IT in the health service means that information once entered can potentially be accessed by a wide range of personnel in the health service and passed on in the same or modified form.

Government proposals for sharing personal data between government departments and for new legislation permitting this pose a

[12] *Inserted by paragraph 1 of Schedule 13 of the Data Protection Act 1998*

very serious threat to patient confidentiality[13].

Statutory Law

The Data Protection Act 1998

The need for confidence in the treatment of personal health data is acknowledged in legislation. Although the words 'patient confidentiality' do not appear on the face of the DPA, personal medical information meets the criteria for a special category of sensitive data, which in theory should provide additional protection for patient records.

The Act requires data controllers, including those holding personal medical information to comply with a range of data protection principles, including the requirement that data only be used for the purposes for which it was collected. However, this principle has been severely modified[14] to permit the use of medical data for other reasons, such as for research purposes.

Data Protection Principle One provides:

'Personal data shall be processed fairly and lawfully....'

The definition of processing includes disclosure of information including oral disclosure from records.

'Lawful' refers both to the requirements found in common law (being a duty not to disclose without consent or unless there is an overriding public interest in disclosure) and with the provisions of Article 8 of the European Convention on Human Rights.

Conditions Justifying Disclosure

Data Protection Principle One goes on to state that personal data

'shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) *in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.'*

(Schedule 3 of the Act has been amended/added to by the Data Protection (Processing of Sensitive Personal Data) Order 2000 SI 2000 417.)

Schedule 2 details a whole host of reasons justifying disclosure in addition to the data subject granting consent. These are where disclosure is necessary:

- for contractual purposes where the data subject is a party e.g. insurance policies, or
- for compliance with legal obligations placed on the data controller (health service bodies are subject to a wide range of legal obligations, many of which could be used to justify disclosure), or
- to protect the vital interests of the subject (which clearly involves the prevention of death or harm of patients), or
- for the exercise of functions of a government department or functions of a public nature exercised in the public interest by any person, or
- for the legitimate interests of the data controller or others.

As well as consent by the data subject, Schedule 3 and the Order also permit disclosure where it is necessary:

- for employment purposes, or
- in the vital interests of the subject, or of another person where consent cannot reasonably be obtained, or
- for the exercise of functions of a government department or functions of a public nature exercised in the public interest by any person, or
- for medical purposes, or
- for insurance and pension purposes (including the use of information about family members), or

[13] Privacy and Data Sharing. The Way Forward for Public Services. Cabinet Office Report.
[14] Section 33 Data Protection Act 1998.

- where there is a substantial public interest in:
  - the detection or prevention or crime, or
  - the protection of members of the public against dishonesty, mal-practice or incompetence, or
  - enabling confidential counselling, or
  - enabling research.

Although the circumstances detailed in these Schedules and in the Order are called conditions, they are in fact exemptions to the prohibition on processing/disclosure of personal data, providing a range of circumstances in which it is legally permissible to disclose identifiable patient information. While obtaining patient consent is one way to secure this information there are many alternative ways of doing so.

The effect is that patient information can be disclosed if the purpose of the disclosure meets just one of the conditions in Schedule 2 and one in Schedule 3 as amended by and added to by SI 2000/417.

It can be seen that disclosure can be made for many reasons without obtaining consent from patients and still be in compliance with the DPA, so long as the information in question was obtained fairly and no breach of the common law is involved. Clearly, almost any activity involving the use and disclosure of medical records could potentially come within these conditions. Although the fair processing requirements – see page 18 - indicate that patients should be told about such disclosures, in practice, they are almost invariably unaware of the uses to which their records are put.

Other Legislative Provisions

Other statutory provisions provide for disclosure of patient information. There are a number of statutes that have limited application, concerning the notification of deaths and infectious diseases and the provision of information to the Driver and Vehicle Licensing Agency about patients who are medically unfit to drive. Similarly, other legislative provisions prohibit disclosure of certain sensitive medical information relating to sexually transmitted diseases, pregnancy terminations and human fertilisation and embryology. The Royal College of Nursing has expressed concern that nurses are being asked to enter information onto NHS databases in breach of the provisions of the legislation providing extra protection to those who have received fertility treatment or treatment for venereal diseases.

Paragraph 36 of the Terms of Service for Doctors[15] places a duty on GPs to respond to requests for patient records from their health authority. The demand of a health authority to see patient records without patient consent was the subject of recent litigation[16] - see page 15.

The Secretary of State for Health has the power to make regulations requiring disclosure of patient records to specified recipients[17]. Those bodies that are asking the Secretary of State to sanction unconsented disclosure of patient records to them include; disease and cancer registries, the Public Health Laboratory, the Health and Safety Executive and medical researchers.

However, the existence of a legislative requirement that information be disclosed without the consent of the patient does not altogether absolve clinicians who do so. They must also be mindful of guidance issued by their own regulatory body and of the human rights of the patient - see page 17.

In view of the confusing state of data protection legislation and the number of exemptions to the requirement to obtain the consent of the data subject that are provided, it is necessary to turn to the common law and Article 8 of the ECHR to establish the safeguards for patient confidentiality.

The Common Law

The notion that there exists a legal right to confidentiality was first enunciated in the case of Prince Albert v Strange in 1849

[15] Schedule 2 of the NHS (General Medical Services) Regulations 1992.
[16] A Health Authority v X and Others [2002]
[17] Section 60 Health and Social Care Act 2001.

where it was recognised that publication or misuse of confidential information may injure a person either emotionally or materially.

In the case of A-G v Guardian Newspapers [1988] Lord Goff summarised the law on confidentiality by saying that 'a duty of confidence arises when confidential information comes to the knowledge of the person (the confidant) in circumstances where he has notice or is held to have agreed that the information is confidential with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others.... The existence of this broad general principle reflects the fact that there is such a public interest in the maintenance of confidences, that the law will provide remedies for their protection.'

When considering the impact of electronic forms of data transmission in the case of R v Brown [1996] Lord Hoffman stated 'The right to keep oneself to oneself, to tell other people that certain things are none of their business, is under technological threat.'

In recent cases the High Court has extended the common law protection for confidentiality to give privacy protection[18] to celebrities.

There have been very few cases concerning breaches of medical privacy. There are reasons for this.

- Patients do not know when information about them is passed on, or who to.
- Even when a patient does become aware of unauthorised disclosure, he or she may be unwilling to make a complaint for fear of jeopardising their relationship with the health professional who has breached their confidence. In particular, patients fear antagonising GPs who have a powerful role as gate keepers to NHS services and who have the right to remove patients from their lists.
- Any patient complaining about unauthorised disclosure of personal information runs the risk that information (which may be particularly sensitive) will be further disseminated in the course of hearing the complaint.

Where the Courts have considered complaints about breaches of patient confidentiality, guidance from the GMC to doctors about their duty of confidentiality to their patients has been considered and approved. The first case concerning an allegation of breach of medical confidence to come before a court was W v Egdell [1990]. It involved disclosure by a doctor of a medical report commissioned by the solicitors for a patient who was held in a secure hospital after having shot and killed five people. W applied for a transfer with view to discharge. Dr Egdell formed the view that W was still a danger to the public and his report stated this. W's solicitors decided not to use this report. Dr Egdell was so concerned about the risk that he felt W posed that he passed a copy of the report to the hospital at which W was detained. A copy was also sent to the Secretary of State and the tribunal. W issued proceedings claiming that Dr Egdell had breached his confidence.

In giving judgement Lord Justice Bingham stated 'It has never been doubted that the circumstances here were such as to impose on Dr Egdell a duty of confidence owed to W. He could not lawfully sell the contents of his report to a newspaper. Nor could he, without a breach of the law as well as professional etiquette, discuss the case in a learned article, or in his memoirs, or in gossiping with friends, unless he took the appropriate steps to conceal the identity of W.'

He went onto to refer to the rule on confidentiality in the GMC rules at the time, which read: *'It is a doctor's duty, except in the cases mentioned below, strictly to observe the rule of professional secrecy, by refraining from disclosing voluntarily to any third party, information about a patient which he has learnt directly or indirectly in his professional capacity as a registered medical practitioner'*. The Court confirmed that this was an accurate statement of the law on confidentiality, while at the same time deciding that the disclosure made by Dr

[18] Naomi Campbell v Mirror Group Newspapers Ltd [2002]

Egdell was sanctioned by the public interest in doing so.

The issue of what amounts to a public interest of sufficient seriousness as to warrant overriding the duty of confidence has also been considered by the courts in other cases. In Woolgar v Chief Constable of Sussex Police & U.K.C.C. [1999], the Court of Appeal considered confidentiality in the context of a statement given to the police by a nurse. Such statements are confidential unless used in the course of a criminal trial. As a general rule confidences should not be broken unless there is an overriding public interest in the disclosure. In this context public interest is considered to be the public good rather than what people may want to know about. The United Kingdom Central Council for Nursing, Midwifery and Health Visiting had requested access to the statement to assist in their investigations into a complaint. The main issue before the court was whether the public interest in respecting confidences was overridden by the public interest in assisting the U.K.C.C. to carry out their disciplinary functions.

The court considered the implications of the fact that the nurse had provided information for one purpose and had not envisaged that it would be passed to the U.K.C.C., nor was she prepared to consent to that disclosure. However, they decided that the countervailing public interest, in permitting a regulatory body access to information to assist them in their investigation of a matter which might affect the safety of patients, was sufficiently serious as to justify the disclosure of the statement to the U.K.C.C.

In a case concerning the use of patient information for commercial purposes the court of Appeal's judgement in R v Department of Health ex parte Source Informatics Ltd. [1999] is of interest. Source Informatics Ltd. wanted to access anonymised patient information from pharmacists to allow them to collate information about GP prescribing habits. They intended to make payment to pharmacists for this information. The Department of Health issued guidance in 1997 in which they advised pharmacists not to release information to commercial concerns. They gave two reasons for this advice. The first was that the process of anonymisation cannot remove the risk that patients may still be identified and secondly that patients had not provided information to their doctors or pharmacists in the expectation that it would be used for such purposes.

The Court of Appeal held that the guidance was unlawful and that although pharmacists are under a duty of confidentiality to patients presenting prescriptions to them for dispensing, they are not under any threat of an action for breach of confidence by passing on anonymised patient data, because;

- anonymised information is not confidential,
- the EU Data Protection Directive does not apply to anonymised information or to the process whereby identifiers are stripped from the data.

Although not a central issue in the judgement, the Court of Appeal indicated that patients cannot be said to impliedly agree to the use of information about them being used for purposes other than for their treatment and care.

The Court of Appeal also considered a case concerning the unauthorised disclosure of a privately commissioned medical report to a patient's GP in the case of Cornelius v Dr de Taranto [2000]. The Court held that damages are payable for distress caused by the unlawful disclosure of a medical report.

In perhaps the most important case to date on the issue of patient confidentiality A Health Authority v Dr X and Others [2001] the Court of Appeal considered a case where the health authority in question believed that GPs, Dr X and his partners, might have breached their Terms of Service. The Authority wanted to investigate the practice in order to establish whether there had been over-dispensing of medicines, inadequate record keeping, poor practice in obtaining patient consent to treatment and inappropriate delegation of responsibility for the medical care of patients. In order to carry out these investigations they believed that they needed access to identifiable patient records.

The GPs, conscious of their duty of confidentiality, sought permission from their patients to release these records. Not all of the patients agreed and some did not respond at all. This placed them in a quandary. The Terms of Service for Doctors requires them to produce records to a health authority on demand, but on the other hand the law and guidance from the General Medical Council requires them to obtain consent from the patient before doing so. On the advice of their legal advisors, the Medical Protection Society they sought clarification from the court.

The case was first heard in the Family Division of the High Court in May 2001. Mr. Justice Munby stressed that disclosure of medical records to a public authority does amount to an interference with that patient's rights under Article 8 of the European Convention on Human Rights and that disclosure can only be justified where;

i. The authority reasonably requires them for its regulatory or administrative functions, and

ii. There is a compelling public interest in their disclosure, and

iii. There are in place effective and adequate safeguards against abuse including safeguards of the particular patient's confidentiality and anonymity.

The Court of Appeal upheld this judgement.

Article 8 of the European Convention on Human Rights

In A Health Authority v X and Others [2002], the court considered the impact of the Human Rights Act 1998. This Act incorporates the European Convention on Human Rights into UK law, including Article 8, which protects privacy. Public authorities including NHS authorities are obliged to operate in accordance not only with the Articles, but also European case law. A case, which typifies the approach of the European Commission and Court of Human rights, is Z v Finland [1997] where the European Court of Human Rights considered a complaint by a woman that her medical records had been seized during an investigation into her husband who was the subject of allegations that he had knowingly exposed people to HIV infection. The complaint was upheld. The Court confirmed that respect for the confidentiality of health data is an important principle to be upheld by all contracting member states and that state measures compelling communication or disclosure without the consent of the patient would be subject to the most careful scrutiny. Z v Finland [1997].

In MS v Sweden [1997] the European Court of Human Rights considered a complaint by a woman who had sought treatment at a clinic. The clinic passed information about her to a government department without her consent. The Court held that information could be disclosed if the law required it to be passed on and there were relevant and sufficient reasons for the disclosure.

It can be seen that the public interest in protecting confidentiality has been accepted by the UK courts. What has been surprising is the scant attention that judges have paid to the Data Protection Act when deciding recent cases. It is clear that what they consider to be of importance is whether any interference with the right to confidentiality can be justified under Article 8 of the European Convention on Human Rights.

Checking whether an Unauthorised Disclosure is Legally Justified

The important factors that the courts are likely to consider when deciding whether disclosures without consent are justified are as follows:

1. Is the information in question of a confidential nature? For example anonymised patient information is less likely to be given legal protection against disclosure.

2. Was the information imparted to the clinician on the understanding that it would not be disclosed, or only disclosed for limited reasons such as for diagnosis treatment and care? Most patients tell their doctors about themselves on the understanding that it will be communicated on a need-to- know basis to others involved in their care.

3. Has guidance issued by the relevant regulatory body (such as the GMC) been complied with?

4. Is there a legal requirement that information be disclosed? There are some legislative provisions requiring disclosure of medical records to health service, government or other bodies – see page 13. However, the existence of such legislation is not conclusive.

5. Is the legislation proportionate to any legitimate objective being sought? If regulations are enacted with the objective of securing access to limited information, but their effect is to require disclosure of entire sets of records, then the courts would be unlikely to uphold its application in cases where the effect is disproportionate. UK courts now have the power to declare secondary legislation to be incompatible with the European Convention and strike it down so as to make it generally unenforceable.

6. Is access reasonably required to permit the body to carry out its legal functions? If there is another way to access the information that is needed, or if anonymised information would suffice, then the courts would be unlikely to sanction unconsented disclosure of patient records.

7. Are there adequate safeguards against abuse? The body seeking access to the records must be able to show that they would protect any information coming into their hands against further unauthorised disclosure.

Courts are likely to balance all these factors in coming to a view. Any clinician or health body considering making disclosures of patient information should carefully consider these points in reaching their decision.

FAIR PROCESSING

Data Protection Principle One requires personal data to be fairly obtained and processed. Part II of Schedule 1 of the DPA provides that fair processing requires that data subjects are told who will hold information about them, what it will be used for and to whom it will be disclosed. These rights are in addition to the right of access detailed in section 7 of the Act.

Duty to Notify Data Subjects of the Existence of Records

Section 7 of the 1998 Act requires data controllers to notify data subjects of the existence of records containing information about them. However, this requirement is only triggered by receipt of a written application. Patients who do not know that a particular institution holds files about them will not be in a position to make such an application. Further, record holders are permitted to avoid the requirement if they hold or have obtained the information in order to comply with legal obligations, or if they can claim that the effort involved in providing this information would be disproportionate. In theory, NHS patients should be told who has been given access to any information that they have disclosed to health professionals. This principle is clearly being breached throughout the NHS.

Part II of Schedule 1 provides that at the time they divulge information about themselves or as soon as possible thereafter, the data controller should ensure that the data subject is told who the information will be held by, for what purpose and to whom it may be passed. Where the information on the record is obtained from a third party, the data subject also has the right to know the source of information. In theory at least, every record holder in the NHS should inform patients that they hold information about them and where that information came from. Consequently, those storing identifiable patient information on databases and those accessing it (such as medical researchers) should tell the patients that they are doing so.

Not surprisingly, the Act provides for wide exemptions from these fair processing requirements. The first is where the provision of this information would involve disproportionate effort. The second, where the information has been passed on to or by the data controller in line with their legal obligations. The Information Commissioner has stated that what amounts to disproportionate effort 'is a question of fact, to be determined in each and every case'. While some disclosures from patient records are made to comply with legal obligations, many more are not. This is an issue on which the NHS has made no comment and those holding and accessing patient records have not been asked to justify their failures to comply with the fair processing requirements.

Preventing the Use of Information

If patients can show that they are being caused substantial unwarranted damage or distress by the use to which personal information about them is being put, they can tell the data processor that they want them to stop storing or using that information[19]. However, they will not be able to enforce their request if they previously consented to the use of the information, or if the processing of the information is necessary to comply with legal obligations or to protect the patient's vital interests.

[19] Section 10 DPA

ENFORCING DATA PROTECTION RIGHTS

Breaches of the access provisions in the DPA, or failures to comply with the data protection principles can be challenged by way of a complaint through the NHS complaints procedure or by complaining to the Information Commissioner or by legal proceedings. Caldicott guardians have a role in overseeing the general uses and protections for records within their health service body but are not charged with responsibility for the confidentiality of individual patient records.

Some failures to comply with the rights of access or to protect patient confidentiality can be pursued by way of a complaint through the NHS complaints procedure. However where there is ambiguity about the law this may not be the most effective way to proceed.

The Information Commissioner's office considers complaints about breaches of the DPA. Section 40 of the DPA provides that the Information Commissioner can issue an enforcement notice on a data controller who has failed to act in accordance with the data protection principles. Failure to comply with an enforcement notice is a criminal offence.

Under the provisions of section 7 of the DPA an application can be made to the courts for an order requiring a data controller to comply with the access provisions. Therefore if a record holder refuses to provide a patient with access to their own medical records, delays in producing them, or levies excessive charges, a court order can be sought. Similarly, if a record holder fails to make corrections to inaccurate records, the courts can be asked to intervene in line with the provisions of section 14 of the Act (automated records) or paragraph 1 of schedule 13 of the Act (manual health records). Section 10 of the DPA also provides that the courts can be asked to require compliance with a notice from a data subject asking the data controller not to continue processing information which is causing substantial damage or distress.

Legal proceedings can also be pursued against data controllers who breach the data protection principles, in particular those who breach patient confidentiality.

Section 13 of the Act provides a right to compensation where damage or distress is caused by a failure on the part of a data controller to comply with their legal obligations. This can be ordered by the courts or by the Information Commissioner.

Complaints to the Information Commissioner should be directed to:

Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF.

Telephone: 01625 545700

e-mail at data@dataprotection.gov.uk

Web site: http://www.dataprotection.gov.uk

particularly where the individual has unique characteristics, which may arise from their medical condition, or the treatment involved.

Some patients may have religious or moral objections to some of the uses of their data in anonymised form. Patients are likely to have interests in the confidentiality of information about them, about which only that only they can judge upon.

The Office of the Information Commissioner considers that anonymisation is difficult to achieve and that where a data controller holds the key to re-anonymisation, the data is still capable of being personal data for the purpose of the Act. Further, she has stated that the process by which data is stripped of personal identifiers amounts to processing and has to be carried out in accordance with the data protection principles[20]. Consequently, those processing or holding anonymised data will need to comply with the DPA unless they only hold effectively anonymised data and have no access a means of re-identifying it.

It is possible that notwithstanding the decision of the Court of Appeal in R v Department of Health ex parte Source Informatics Ltd. 1999, heard prior to the introduction of the Human Rights Act, a court might now be prepared to use Article 8 of the ECHR to regulate the use of anonymised information.

Medical Reports for Insurance and Employment Purposes

Applications for access to medical reports prepared for insurance or employment purposes are still covered by the provisions of the Access to Medical Reports Act 1988. This requires the consent of the patient before the report can be prepared and supplied to the commissioning employer or insurer.

CHCS - COMPLIANCE WITH THE DATA PROTECTION ACT

For the purposes of the records that they hold, CHCs are data controllers and must register with the office of the Information Commissioner and comply with the provisions of the data protection legislation. Registration and compliance advice is available on the Information Commissioner's website at http://www.dataprotection.gov.uk

CHCs must remember that they are required to give their clients access to their records and comply with all the data protection principles reproduced at appendix 1.

Practical steps that CHCs should take, include:

1. Providing all clients with a statement about how the CHC deals with and protects the information they impart.

2. Ensuring that client consent is obtained before information about them is shared or otherwise divulged.

3. Retain records for no longer than is necessary. See Appendix to HSC 1999/053 for retention periods.

[20] Data Protection Act 1998 Legal Guidance.

APPENDIX 1 - THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

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

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

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

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

7. 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.

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.

Crown copyright. Reproduced with permission of the Controller of her Majesty's Stationery Office.

FURTHER READING

1. The Data Protection Act 1998 Legal Guidance Issued by the Office of the Information Commissioner and available at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf

2. Subject Access and Third Party Information. Guidance issued by the Office of the Information Commissioner also available at http://www.dataprotection.gov.uk/dpr/dpdoc.nsf

3. Clinical Confidentiality. Charles Foster and Nicholas Peacock Monitor Press 2000

4. Patient Confidentiality and Caldicott Guardians- Frequently Asked Questions Department of Health publication October 2001 available at http://www.doh.gov.uk/ipu/confiden/faq.htm#THE%20COMPLAINTS%20PROCEDURE

5. Privacy and Data Sharing. The way forward for public services. Cabinet Office report April 2002 available at http://www.piu.gov.uk/2002/privacy/report/index.htm

BIBLIOGRAPHY

1. Access to Health Information John Halford and Jean Gould published in two parts in the Journal of the Legal Action Group in March and September 2001.

2. The EC Data Protection Directive 1995: An Analysis. Freddy Kosten and Dr Chris Pounder Web Journal of Current Legal Issues 1996.

3. Access to Health Records. The Legal Requirements. ACHCEW March 1998.

4. The Data Protection Act 1998. Implications for Patients' Rights – A Briefing Paper. ACHCEW March 1999.

5. The Protection and Use of Patient Information. Department of Health. March 1996

6. Data Protection Act 1998 Protection and Use of Patient Information Issued under HSC 2000/009

7. Confidentiality: Protecting and Providing Patient Information. General Medical Council. September 2000. Available at http://www.gmc-uk.org/standards/standards_frameset.htm

8. Caldicott Committee. Report on the Review of Patient Identifiable Information. Department of Health 1997

9. Legal and Policy Constraints on Electronic Records. Requirements Report. Department of Health Information Policy Unit March 2002

£2.50 (p&p inc.)
ISBN: 0-9542478-1-7

Published by:
The Association of Community Health Councils for England & Wales
30 Drayton Park, London, N5 1PB
www.achcew.org.uk e-mail: mailbox@achcew.org.uk