USE AND DISCLOSURE OF HEALTH DATA


May 2002
Table of Contents

Information Commissioner’s Foreword

Chapter 1: Introduction

Chapter 2: First Data Protection Principle
- Schedule 2 & Schedule 3
- The fair collection of personal data
- Lawful processing

Chapter 3: Second Data Protection Principle
- Section 33 Research Exemption

Chapter 4: Confidentiality
- Consent
- The Commissioner’s approach

Chapter 5: The Right to Object to Processing
- Opt-outs
- Section 10 Notices

Appendix 1: Practical Application
- Examples of Uses and Disclosures

Appendix 2: Glossary of Terms

Appendix 3: Schedule 2 and Schedule 3 Conditions
Information Commissioner’s Foreword

The Data Protection Act 1998 presents a number of significant challenges to data controllers in the health sector. Over the course of the last year, I have seen a significant increase in the number of requests for assistance from individuals. At the same time I have been asked to consider issues arising out the Department of Health electronic patient records project, issues in relation to cancer and other disease registries, and issues in relation to the use of patient data in research. Frequently these requests for advice have significant implications for the NHS as a whole and the Department of Health as well as for patients.

It seems to me that there are several reasons for the increase in requests for assistance and advice. Firstly there has been an extension of the scope of Data Protection from purely automated records to many classes of manual records. Whereas the 1984 Act only applied to computerised records, the 1998 Act applies fully to all patient records whether they are held on computer or in paper files, and whether they consist of hand written case notes or x-rays.

Secondly, it is clear that many practitioners are confused between the requirements of the Data Protection Act and those of the various regulatory and representative bodies within the sector including the GMC, MRC, and BMA. To some extent the advice issued by these different bodies may reflect their different roles. To some extent it may also reflect misunderstandings of the requirements of the Act. It is a common misconception, for instance, that the Act always requires the consent of data subjects to the processing of their data. At the same time, as private litigation increases throughout society, many health service bodies have adopted a more cautious approach towards the use and disclosure of patient data, fearing that uses and disclosures of data which previously seemed unexceptionable might attract action for a breach of confidence.

Thirdly, the demands that are placed on the health service are greater and more varied than ever before. Health Authorities, NHS Trusts and individual practitioners are increasingly involved in inter-agency initiatives, whether in the context of the Crime and Disorder Act or the joint delivery of health and social care with local authority social service departments. Meanwhile, the creation of a national system of electronic health records is likely to raise fresh questions about who is responsible for those records and who should be allowed access to them.

If steps are not taken to clarify the ground rules, then the uncertainty experienced by clinicians and NHS organisations may translate into concerns on the part of patients as to who has access to their records and on what basis their personal data are processed. In that context I welcome wholeheartedly statements by Department of Health Ministers that in the foreseeable future all processing of patient records should be on the basis of informed consent. I also welcome the decision of the NHS Executive to begin work on development of a Code of Practice that is aimed at producing coherent practical guidance for clinicians and health service bodies incorporating the different standards emanating from the different professional and representative bodies. The guidance that I have published is more limited in its ambition. My aim has been to clarify the minimum requirements of the Data Protection Act, providing answers to frequently asked questions such as:

- Is patient consent necessary for processing?
- If so, in what circumstances?
- If so, in what form?
- When is it necessary to anonymise data?
- When is it necessary to pseudonymise data?
Although as far as possible the Guidance attempts to provide practical examples of the steps that should be taken in order to achieve compliance with the requirements of the Act, the audience for the Guidance is not primarily practitioners but data protection officers, Caldicott Guardians and those charged with the development of the IT infrastructure of the NHS. It is, in other words a somewhat technical document that seeks to explain the enforceable requirements of the Data Protection Act rather than to describe “good practice”.

The term “enforceable requirements” refers to the powers given to me by the Act to take action against data controllers whom I consider to be in breach of any of the eight Data Protection Principles in Schedule 1 of the Act. The Act does not, however, require that I take enforcement action on each occasion that I consider that there has been a breach. Before serving an enforcement notice I will not only measure the performance of the data controller against the standard set out in the guidance but also consider, as the Act requires, whether the actions of the data controller have caused damage or distress to any individual. I shall also have regard to the circumstances of different data controllers. For instance, as is explained in the section of the Guidance dealing with privacy enhancing technologies, in many cases it may be possible to process patient data, for instance for research or administrative purposes, without having access to the data which would identify particular patients. While I would not necessarily expect each GP practice to develop its own IT system capable of concealing the identities of patients from those who do not need to know them, I do expect those developing IT systems for use by GPs to build in such a capability and I would certainly consider action against a GP (or any other data controller) who did not make use of the features available on a system for maximising the privacy of patients.

Finally, I would like to thank all those who have contributed towards the development of this guidance. Some seventy responses were received to the initial consultation paper issued in May 2001. Since a number of these were received from representative bodies, the number of organisations who had input was actually much greater. I would also particularly like to thank those individuals and organisations who attended the consultative seminar which I held in October of last year. While there will inevitably be issues upon which I am asked to provide further clarification, I am certain that without the help of all those who contributed to the consultation I would have faced a far greater number of such requests.

Elizabeth France
May 2002
Chapter 1: Introduction

Scope of the Guidance

The Data Protection Act 1998 gives effect in UK law to EC Directive 95/46/EC, and introduces Eight Data Protection Principles that set out standards of information handling. These standards apply to all data controllers who process personal data. This guidance is concerned with the application of the Act with regards to the processing of information contained within ‘health records’. The term, “Processing”, includes the collection, use, and disclosure of personal data. The guidance is limited, in the main, to the requirements of the First Data Protection Principle and the Second Data Protection Principle. Further general advice regarding the other Principles, which cover such matters as data quality, rights of access, and security, can be found in “The Data Protection Act 1998 – Legal Guidance”, which is available on the Information Commissioner’s website at [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk).

The term ‘health record’ is defined by Section 68 of the Act, and means any record which:

- consists of information relating to the physical or mental health or condition of an individual, and
- has been made by or on behalf of a health professional in connection with the care of that individual.

The term ‘health professional’ is also defined by the Act, and the definition is included in Appendix 2.

This Guidance will be of most value to individuals within organisations (including both the public and private sector) whose responsibilities include data protection, privacy and confidentiality issues. These may include data protection officers, Caldicott Guardians, or legal advisers. The Guidance sets out the requirements of the law and in some cases provides an indication of the issues that data controllers will need to consider when fulfilling their obligations under the Act. The Guidance also aims to provide an indication of the standard which the Information Commissioner will seek to enforce. It is not the intention of this Guidance to provide specific advice on all the possible uses and disclosures of patient information. Data controllers will need to apply the general advice provided here to their specific situations. Box 1 gives an indication of the areas upon which guidance is provided. These are treated more fully in Appendix 1.
Examples of uses and disclosures of personal data

a) Care & Treatment
   • Routine record keeping, consultation of records etc, in the course of the provision of care and treatment;
   • Processing of records in the event of a medical emergency;
   • Disclosures made by one health professional or organisation to another, e.g. where a GP refers a patient to a specialist;
   • Clinical audit e.g. the monitoring of a patient care pathway against existing standards and benchmarks.

b) Administration
   • Processing for administrative purposes, e.g. disclosure by a GP made in order to receive payment for treatment provided;
   • Administrative audit, which may include studies designed to improve the efficiency of the NHS as an organisation, e.g. to support decisions about the allocation of resources.

c) Research & Teaching
   • Statutory disclosures to disease registries and for epidemiological research;
   • Non-statutory disclosures to disease registries and for epidemiological research;
   • Clinical trials;
   • Hospital-based teaching;
   • University-based teaching.

d) Use and disclosures for non-health purposes
   • Disclosures for Crime and Disorder Act 1998 purposes;
   • Disclosures to the police;
   • Disclosures to hospital chaplains;
   • Disclosures to the media.

This list is not exhaustive. It is likely that data controllers will need to apply the requirements of the Act to uses and disclosures of health data that are not listed above.
Chapter 2: First Data Protection Principle

The First Data Protection Principle states:

“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”

The conditions in Schedules 2 and 3, referred to above, are listed in Appendix 2.

It is possible to identify a number of separate, albeit cumulative, requirements of this Principle:

- The requirement to satisfy a condition in Schedule 2 and Schedule 3;
- The requirement to collect personal data fairly;
- The requirement to process personal data lawfully.

The requirement to satisfy a condition in Schedule 2 and Schedule 3

In all cases data controllers must satisfy at least one of the conditions in Schedule 2 of the Act. In the context of health sector data controllers, the most relevant Schedule 2 conditions are likely to be:

- Processing with the consent of the data subject;
- Processing necessary to protect the vital interests of the data subject;
- Processing which is necessary for the exercise of functions of a public nature exercised in the public interest by any person;
- Processing which is necessary for the purposes of the legitimate interests pursued by the data controller or those of a third party to whom the data are disclosed, except where the processing is prejudicial to the rights and freedoms or legitimate interests of the data subject.

In practice, it is unlikely to be difficult to satisfy one of these conditions. The focus of this section of the Guidance is therefore on the Schedule 3 processing conditions, at least one of which must be satisfied when processing sensitive personal data. “Sensitive data” is defined in the Act and includes data that relates to the physical or mental health of data subjects. No distinction is drawn in the Act between, say, data relating to the mental health of patients and data relating to minor physical injuries: they are all sensitive.

The most relevant Schedule 3 conditions are likely to be:

- Processing with the explicit consent of the data subject;
- Processing necessary to protect the vital interests of the data subject or another person, where it is not possible to get consent;
- Processing necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights;
- The processing is necessary for medical purposes and is undertaken by a health professional or a person owing a duty of confidentiality equivalent to that owed by a health professional.

The Act provides that included within the term ‘medical purposes’ are preventative medicine, medical diagnosis, medical research, the provision of care and treatment, and the management of healthcare services. This definition, with the exception of medical research, is taken from the
Directive from which the Act is derived. The Commissioner considers that the term ‘vital interests’ refers to matters of life and death.

The Schedule 3 conditions have been supplemented by further conditions set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000. The most likely conditions for the purposes of this Guidance are:

- Processing of medical data or data relating to ethnic origin for monitoring purposes;
- Processing in the substantial public interest, necessary for the purpose of research whose object is not to support decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject and which is unlikely to cause substantial damage or substantial distress to the data subject or any other person.

The Necessity Test

Many of the conditions for processing set out in Schedule 2 and Schedule 3 specify that processing must be necessary for the purpose stated. In order to satisfy one of the conditions other than processing with consent, data controllers must be able to show that it would not be possible to achieve their purposes with a reasonable degree of ease without the processing of personal data. Where data controllers are able to achieve, with a reasonable degree of ease, a purpose using data from which the personal identifiers have been removed, this is the course of action that they must pursue. This may require the use of Privacy Enhancing Technologies (PETs) – Box below. What constitutes a ‘reasonable degree of ease’ is to be determined by taking into consideration issues including the technology available, and the form in which the personal data are held.

The Commissioner takes the view that when considering the issue of necessity, data controllers must consider objectively whether:

- Such purposes can be achieved only by the processing of personal data; and
- The processing is proportionate to the aim pursued.

This aspect of the First Principle is reinforced by the Third Data Protection Principle, which states that:

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

The disclosure of personal data where this is not actually necessary would be likely to contravene this Principle.
Privacy Enhancing Technologies (PETs)

In a general sense, the term “PET” is used to refer to an IT design philosophy which seeks to deploy new technology in ways which enhance rather than undermine privacy. From this standpoint, the use of techniques such as encryption, password control and other measures designed to ensure that data are guarded with appropriate security can all be regarded as privacy enhancing technologies. Privacy, however, is not limited to security and confidentiality. A Privacy Enhancing approach to database design might allow the holding of patient preferences (e.g. consent to be contacted in connection with medical research), might prompt a clinician to check the personal details of a patient who has not visited a surgery for some years, and might force the periodic review of older records.

More specifically PETs have become associated with systems designed to protect the identity of patients by substituting true identifiers such as name, address or National Health Number with pseudonyms. The starting point is the implied requirement of Schedule 2 and 3 of the Act that, in the absence of consent, personal data should only be processed where it is necessary to do so. If it is never necessary to know the identity of the individuals to whom personal data relates, then the data should be anonymised by removing all personal identifiers. Anonymisation is a permanent process and once anonymised, it will never be possible to link the data to particular individuals.

However, permanent anonymisation may not always be acceptable. For instance a researcher may have no need to know the identity of the patients suffering from a particular condition. He or she may, however, need to know that the patient who was diagnosed with the condition on a particular date is the same patient who was diagnosed with a different condition on another date. Pseudonymisation, sometimes described as “reversible anonymisation” provides a solution. In effect a computer system is used to substitute true patient identifiers with pseudonyms. The true identities are not, however, discarded but retained in a secure part of the computer system allowing the original data to be reconstituted as and when this is required. Typically those making day-to-day uses of pseudonymised data would not have the “keys” allowing the data to be reconstituted.

Potentially there are many different applications for such PETs. For instance they might allow researchers to make more extensive use of medical records without increasing the risk of the misuse or accidental disclosure of patient details. They might prevent support staff from gaining access to information about the medical condition of patients while allowing access to the information necessary to perform administrative tasks.

The Commissioner expects that consideration will be given to the deployment of PETs in all significant new IT developments within the Health Service. She would also expect that data controllers within the Health Service make use of any privacy enhancing features of the software and hardware which they use.
The requirement to collect personal data fairly

The Data Protection Principles are listed in Part 1 of Schedule 1 of the Act. Part 2 of Schedule 1 contains further statutory interpretation of the Act. Paragraph 2 of Part 2 sets out the obligation on data controllers to provide certain information to data subjects when collecting their personal data:

- The identity of the data controller;
- The identity of any representative nominated by the data controller for the purposes of the Act;
- The purpose or purposes for which the data are to be processed; and
- Any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable the processing in respect of the data subject to be fair.

These details are often referred to as “fair processing information”, “the fair processing code”, or the “fair collection code”. In this Guidance we refer to these details as “fair processing information”.

The question of the nominated representative of the data controller is highly unlikely to arise in the context of health records, and is not therefore considered here. The other three requirements are considered separately, before discussing the timing and the level of detail to be provided.

Identity of the data controller

Care should be taken to ensure that the data subject knows the identity of the data controller(s) that will process his or her data. Information as to the identity of the data controller should be reasonably specific (e.g. a GPs practice, a NHS Trust etc). “The NHS” or “The Health Service” are not legal entities and therefore cannot be data controllers. Within a GP practice the assumption of data subjects is probably that the practice as a whole is the data controller and that other members of the practice may have access to their records. If there is any doubt, e.g. if a number of GP practices share the same premises, it is the duty of the GP practice to ensure that the patient knows the true position.

Data controllers must also be aware that with increased multi-agency working and initiatives (e.g. between a Trust and a social services department), it may not be immediately clear to data subjects as to who the data controller actually is. Indeed, there may be more than one data controller, in which case the identity of all data controllers should be communicated to data subjects.

Purpose or purposes of processing

When explaining the purpose or purposes for which information is to be processed, data controllers must strike a balance between providing an unnecessary amount of detail and providing information in too general terms. An explanation to the effect that personal data are to be processed for ‘health care purposes’ would be too general. On the other hand, an explanation that explained all the administrative systems in which patient data might be recorded, the use of data for diagnosis, for treatment etc would be excessive. (An explanation which is not sufficiently detailed is unlikely, in any event, to be sufficient to obtain the consent of the data subject to the processing of data should this be required. The question of consent is considered in more detail in Chapter 4).
Other information necessary to make the processing fair

The Act provides no guidance as to what further information should be provided to data subjects in order to make the processing of their data fair. Clearly this will vary from case to case and from patient to patient depending upon levels of understanding of how the NHS operates, command of English and the sensitivity of the data in question. However, among the information that it may be necessary to provide is the following:

- Information as to what data are to be or have been recorded, where this is in doubt. Patients are likely to expect that basic information will be recorded as to diagnosis and treatment. They may, however, be surprised to find that other information has been recorded whether this is an opinion of a doctor or the circumstances surrounding an injury. Unless patients have a reasonably clear idea of what is recorded about them, any consent to other uses or disclosures of their data may not be valid.

- Information as to specific disclosures. Given the sensitivity of medical data, data subjects should be informed of any non-routine disclosures of their data.

- Information as to whether any secondary uses or disclosures of data are optional. Where patients have a choice as to whether to provide information, to allow its disclosure to third parties or to object to certain uses or disclosures, then the requirement of fairness suggests that these choices should be brought to their attention.

How much fair processing information should be provided?

Concern has been expressed that the fair processing rules may require the provision of very large amounts of information in which patients have no real interest. In the Commissioner’s view this concern is misplaced. In effect the fair processing information provided should achieve two basic purposes:

- It should provide sufficient information to allow the patients to exercise their rights in relation to their data. Hence patients should be told who will process their data, including any disclosures of personal data (which will allow them to make subject access requests), whether it must be supplied (which will allow them to opt-out if they wish), and what information is contained in their record (which will allow them to give meaningful consent to its processing.)

- It should provide sufficient information to allow the individual to assess the risks to him or her in providing their data, in consenting to their wider use, in choosing not to object to their processing etc. This should have at least two consequences for data controllers. It should become clear that fair processing notices do not need to contain a large amount of detail about routine, administrative uses of data. It should also become clear that researchers engaged in open-ended studies are not prevented by the Act from soliciting patient data on the grounds that their fair processing notices cannot be sufficiently detailed. Fair processing notices in this case should simply need to make clear that the research in question is indeed open-ended, leaving the individual to assess the risk.

It may also be helpful to bear in mind that the fair processing rules do not mean that patients must be provided with information that they are known to already possess.
When should fair processing information be provided?

It is likely that there will be a number of standard purposes for which the personal data of all patients entering a hospital or registering with a GP will be processed, information about which can be provided to patients at the outset of the episode of care. In particular, patients may need to be told about typical flows of data between different NHS bodies. This information is relatively timeless and it is appropriate that patients are given it at an early opportunity. It would certainly be good practice to remind patients of this information from time to time, for instance by ensuring that leaflets containing the relevant information are available to patients.

Some patients may subsequently have their personal data processed for a number of additional purposes e.g. information about a cancer diagnosis may be passed to a cancer registry, or information may be passed to social services. Those patients who will have their personal data processed for these additional purposes will need to be provided with this further information, in order to satisfy the fair processing requirements. This type of information is specific to particular patients at particular times and should be given in context, at a time when individuals are able to make sense of it.

How should the fair processing information be given?

The provision of ‘fair processing information’ by means of a poster in the surgery or waiting room or by a notice in the local paper etc is unlikely to be sufficient to meet the requirements of the Act since not all patients will see or be able to understand such information. Such methods may, however, be used to supplement other forms of communication. Methods by which the fair processing information may be provided include a standard information leaflet, information provided face to face in the course of a consultation, information included with an appointment letter from a hospital or clinic, or a letter sent to a patient’s home. The effort involved in providing this information may be minimised by integrating the process with existing procedures. Many GP practices, for instance, already provide leaflets to patients about how the practice operates. Such leaflets could easily incorporate the fair processing information. Doctors may be able to easily provide specific information to patients in the course of consultations. Only where such an opportunity does not present itself will it be necessary to contact patients separately, for instance, if they are to be invited to participate in a programme of research involving the disclosure of their medical records to a researcher who may wish to interview patients with particular medical conditions.

Obtaining data from a person other than the data subject

In many cases medical information will be obtained directly from the patient either because it has been supplied by the patient (e.g. a description of symptoms) or has been obtained by a medical examination conducted by the person creating the record (e.g. an observation of symptoms). In a significant proportion of cases, however, data will be obtained by other means, whether from a third party or generated by the person creating the record (e.g. a medical opinion based on symptoms presented).

The Act recognises that the provision of fair processing information when data are obtained other than from the data subject presents some difficulties. The following exceptions from the provision of the fair processing information may only be relied upon by data controllers where they have obtained personal data from someone other than the data subject. It should be stressed that the
ability to rely on an exemption does not absolve the data controller from the overriding duty to process personal data fairly.

The exceptions are:

- Where providing the fair processing information would involve a disproportionate effort; or
- Where it is necessary for the data controller to record the information to be contained in the data, or to disclose the data, to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

The term ‘disproportionate effort’ is not defined by the Act. In assessing what does or does not amount to disproportionate effort, the starting point must be that data controllers are not generally exempt from providing the fair processing information because they have not obtained data directly from the data subject. What does or does not amount to disproportionate effort is a question of fact to be determined in each and every case.

In deciding this, the Commissioner will take into account a number of factors, including the nature of the data, the length of time and the cost involved to the data controller in providing the information. The fact that the data controller has had to expend a substantial amount of effort and/or cost in providing the information does not necessarily mean that the Commissioner will reach the decision that the data controller can legitimately rely upon the disproportionate effort exception. In certain circumstances, the Commissioner would consider that such an effort could reasonably be expected. The above factors will always be balanced against the effect on the data subject and in this respect a relevant consideration would be the extent to which the data subject already knows about the processing of his or her personal data by the data controller.

Data controllers should note that the Data Protection (Conditions Under Paragraph 3 of Part II of Schedule 1) Order 2000 provides that any data controller claiming the benefit of the disapplication of the requirement to provide fair processing information must still provide this information to any individual who requests it. In addition a data controller who does not provide fair processing information because to do so would involve disproportionate effort must keep a record of the reasons why he believes the disapplication of the fair processing requirements is necessary.

In practice, the Commissioner thinks that it is increasingly unlikely that NHS data controllers will be able to rely successfully upon these provisions. While there will be many cases in which, say, a consultant, receives personal data from a person other than the data subject, for instance his or her GP, the GP will have obtained the data directly from the patient and will have therefore provided the necessary fair processing information. There is no need, in other words, for the consultant to rely upon the exception since the patient will already be in possession of the fair processing information.

One area, however, where the exception is likely to be of assistance is that of records created before the enactment of data protection legislation. The Commissioner would generally accept that it would involve disproportionate effort to write to all existing patients to provide the fair processing information. However, that information should be available to patients when they attend surgeries and clinics and would have to be given in the event of any non-routine uses or disclosures of personal data.

The exception may also be relevant for those carrying out records based research where records were created in the past without the intention of using them for research purposes. (This issue is considered in greater detail in the following chapter under the heading “The Research Exemption”.)
Cases where the requirement to provide fair processing information does not apply

There are a number of circumstances in which the requirement to provide the fair processing information does not apply.

- Section 29 of the Act permits uses or disclosures of personal data for the purpose of the prevention or detection of crime or the prosecution or apprehension of offenders, even though the data subject was not informed of those uses or disclosures, if to inform the data subject might prejudice that purpose. This may be of relevance in the context of combating fraud and corruption, e.g. in circumstances where it may be alleged that a GP has sought payment from a Health Authority for treatment which was not given, or where it is alleged that a patient has claimed free treatment to which he or she is not entitled. The exemption may also justify the disclosure of medical information to the police investigating an alleged assault on a member of staff.

- Section 31(2)(a)(iii) of the Act may allow for the disclosure of personal data without a prior explanation having been given to the data subject if the disclosure is necessary for protecting members of the public against “dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or activity”. This would appear to allow disclosures, in certain cases, of patient data to bodies responsible for maintaining professional standards.

- Section 31(4)(iii) allows the disclosure of personal data to the Health Service Commissioners (the Ombudsman) if not to do so would prejudice the discharge of the functions of those bodies.

- Section 35 allows the disclosure of information without breach of, among other things, the First, Second and Third Principles where the disclosure is a requirement of law or for the purpose of establishing, exercising or defending legal rights.

Although the exemptions may be relevant in some cases, they are unlikely to be the basis for the routine or wholesale processing of data without the provision of the information specified in the fair processing information to the data subject. In many cases, even though an exemption is apparently available, it would be wrong to rely upon it since it would be unnecessary to do so.

An example would be a disclosure of personal data for medical research purposes made in accordance with an order under s.60 of the Health and Social Care Act 2001 (applicable only in England and Wales). An order might specify, for instance, that all clinicians making a diagnosis of cancer must make a report to a cancer registry. While superficially s.35 suggests that fair processing information need not be given to the patient since the disclosure is a requirement of the law, in fact it would not be proper to rely upon the exemption since to provide the fair processing information would not be inconsistent with the disclosure.

By contrast, a hospital might decide to disclose to the police relevant parts of the medical record of a patient who had assaulted a member of staff even though no fair processing information had been given, since in that case there would be prejudice to the s.29 purpose of the disclosure if the normal rules were followed.

The requirement to process personal data lawfully

In addition to the requirement to satisfy a condition in Schedule 2 and Schedule 3 of the Act, there is a general requirement that personal data are processed lawfully. While the Act does not provide any guidance on the meaning of the terms “lawful” or “unlawful”, the natural meaning of unlawful has been broadly described by the Courts as “something which is contrary to some law or
enactment or is done without lawful justification or excuse”. In effect, the Principle means that a
data controller must comply with all relevant rules of law whether derived from statute or common
law, relating to the purpose and ways in which the data controller processes personal data. The
following may be relevant when deciding whether personal data have been processed lawfully:

- **Statutory prohibitions on use or disclosure:** If the general law prevents a particular
disclosure of personal data then there would also be a contravention of the lawful
processing requirement of the Data Protection Act 1998 if a disclosure were made.

- **The ultra vires rule and the rule relating to the excess of delegated powers,** under which the
data controller may only act within the limits of its legal powers: Public authorities such as
the Department of Health or a NHS Trust might exceed their powers if, for instance, they
were to make commercial use of patient data, e.g. by selling names and addresses to the
manufacturers of medical equipment.

- **Contractual restrictions on processing:** this may be of particular relevance in the private
health sector where the provision of treatment is on the basis of a contract between the
patient and the clinician, clinic, hospital etc.

- **Confidentiality arising from the relationship of the data controller with the data subject:** this
issue is considered separately in Chapter 4.

- **Article 8 of the European Convention on Human Rights (the right to respect for private
and family life, home and correspondence):** the Human Rights Act 2000 underpins the
Data Protection Act and other legislation. Public authorities are required to construe the
legislation under which they operate in accordance with the European Convention on
Human Rights and to ensure that their actions and those of their staff are consistent with it.

This list is by no means exhaustive. The various different considerations inevitably overlap. The
key issue for the processing of health data is likely to be the common law duty of confidence. This
is addressed in greater detail in Chapter 4. In brief, even though the Act does not explicitly require
the consent of patients in order to process medical data, in many cases there is an implied
requirement to obtain patient consent for the processing of data since to process without consent
would involve a breach of a duty of confidence which, in turn, would involve a breach of the
requirement in the Act to process personal data lawfully.
Chapter 3: The Second Data Protection Principle

The Second Data Protection Principle states:

“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 those purposes.”

There are two means by which a data controller may specify the purpose or purposes for which the personal data are obtained:

- In a notice given by the data controller to the data subject in accordance with the fair processing requirements; or
- By notifying the purposes on a data controller’s Data Protection Register entry, through the Notification procedures. (It should be noted that Notification to the Commissioner alone will not satisfy the fairness requirements of the First Principle).

These are cumulative and, except in cases where it is proposed to process personal data for purposes that were not envisaged at the time of collection, the information provided to the data subject will reflect the purposes notified to the Commissioner. The effect of the Principle is to reinforce the First Principle and also to limit the range of cases where data may be processed for purposes of which the data subject was not informed to ones which are compatible with those for which data were originally obtained.

The Research Exemption

The Act does envisage some exceptions to the Second Principle, notably where personal data are processed for the purposes of research (including statistical or historical purposes). These exceptions are set out in Section 33 of the Act, which is commonly known as ‘the research exemption’. These exceptions can be applied where the processing (or further processing) is only for research purposes, and where the following conditions are met:

- The data are not processed to support measures or decisions relating to particular individuals; and
- The data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Where the exemption applies:

- The further processing of personal data will not be considered incompatible with the purposes for which they were obtained. (It is important to note that the exemption does not excuse the data controller from complying with the part of the Second Principle that states that personal data shall be obtained only for one or more specified and lawful purposes);
- Personal data may be kept indefinitely (despite the Fifth Data Protection Principle which states that personal data should not be kept for longer than is necessary);
- Subject access does not have to be given provided that the results of the research or any resulting statistics are not made available in a form that identifies the data subject.

It is important to note that even where the exemption applies, the data controller is still required to comply with the rest of the Act, including the First and Second Principles. The data controller should ensure that at the time the data are collected, the data subject is made fully aware of what
the data controller intends to do with the data. If the data controller subsequently decides to process the data in order to carry out further research of a kind that would not have been envisaged by the data subject at the time the data were collected, the data controller will need to comply with the fair processing requirements of the Act in respect of this processing.

The exemption cannot be used to justify the retention of records for longer than would normally be the case simply because the records might be used for research in the future. The exemption may only be used, in other words, if research is actually being carried out or there is a firm intention to use the records for that purpose.

The research exemption, combined with the special fair processing rules in relation to data obtained from someone other than the data subject, has implications for records based research. Two general cases may be distinguished. In the first case, it is proposed to conduct records based research by making use of current records or ones yet to be created. Patients should be informed, as part of the standard fair processing information, that their data may be used for research purposes designed to better understand and treat their conditions. The research exemption (insofar as compatibility with the Second Principle is concerned) is not relevant since these records will have been compiled both for the purpose of treatment and research.

In the second case, research is proposed using existing records of patients who are no longer being treated for their condition. Such records may be quite old. Those patients who may be contacted without involving disproportionate effort should be given fair processing information. Those patients who cannot be contacted without disproportionate effort need not be given the fair processing information although the researcher should record this fact. The research exemption permits the use of these data for research, providing that the conditions described above apply.
Chapter 4: Confidentiality

Chapter 2 considered, among other matters, the general requirement to process personal data lawfully. While there are potentially a large number of considerations which data controllers processing health data must take, in practice, the key issue in this context is likely to be the duty of confidence.

The duty of confidence is a common law concept rather than a statutory requirement. As such it derives from cases that have been considered by the Courts. Inevitably there are areas which have not been litigated, where it is impossible to state with any certainty whether a duty of confidence exists and, therefore, that the consent of patients is required for the processing of their data. Even where there is case law, it may be difficult to extrapolate general principles from the particular circumstances of the case. There is no certainty that a decision made many years ago by a court would be reflected in a decision made in the context of a modern NHS. In this chapter, we first provide a general introduction to the concept of confidentiality, its exceptions and the requirement to obtain the consent of patients for the processing of medical data. Then we attempt to describe the approach taken by the Commissioner in the area of health.

Confidentiality & Exceptions to the Duty of Confidence

Personal data that are subject to a duty of confidence have a number of characteristics:

- The information is not in the public domain or readily available from another source;
- The information is of a certain degree of sensitivity, (more than “mere tittle tattle”) such as medical data;
- The information has been provided with the expectation that it will only be used or disclosed for particular purposes. This expectation may arise because a specific undertaking has been given, because the confider places specific restrictions on the use of data which are agreed by the recipient, or because the relationship between the recipient and the data subject generally gives rise to an expectation of confidentiality, for instance as arises between a customer and a bank or a patient and a doctor.

The Courts have generally recognised three exceptions to the duty of confidence:

- Where there is a legal compulsion;
- Where there is an overriding duty to the public;
- Where the individual to whom the information relates has consented.

Certain disclosures of medical data have long been requirements of the law. Certain diseases are notifiable. More recently s.60 of the Health and Social Care Act 2001 creates a power for the Secretary of State to make orders (subject to various safeguards, and only applicable in England and Wales) requiring the disclosure of patient data that would otherwise be prevented by a duty of confidence. Courts may order the disclosure of patient data in particular cases.

Disclosures required by law are relatively easy to identify. Disclosures that may be justified as being in the public interest, by contrast, necessarily involve the exercise of judgment, balancing the rights of patients against the public good. For instance, a hospital may consider the disclosure of medical information to the police would be justified in the event of an assault on a member of staff but unjustified in the context of a minor theft. Because such decisions involve the exercise of judgment it is important that they are taken at an appropriate level and that sound procedures are developed for taking those decisions.
Consent

Most uses or disclosures of medical data will be justified by having obtained the consent of patients. There is no single definition of consent.

The EU Directive, for instance, defines consent as: “…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.” On one reading this definition suggests that the giving of consent may not legitimately be made a condition of receiving a service such as health care since to impose conditions might mean that consent had not been “freely given”. Were a data controller to seek to rely upon consent as a condition of processing medical data (rather than one of the other possible conditions suggested in Chapter 2) such a strict reading of the definition in the Directive might invalidate the consent that had apparently been obtained.

In considering the common law duty of confidence, however, the courts have not generally found that consent is rendered invalid by having conditions attached, providing that those conditions are not unduly onerous. In considering the common law duty of confidence, it is this approach to consent that the Commissioner will follow, taking three key considerations.

Firstly, consent must be informed. The data subject must know, in other words, what are the proposed uses or disclosures of personal data. In effect a patient will be able to give informed consent if he or she has been supplied with the fair processing information discussed earlier. It follows from this that a patient cannot be deemed to have consented to something of which he or she is ignorant.

Secondly, the person giving consent must have some degree of choice. “Consent” given under duress or coercion is not consent at all. By contrast consent which is entirely optional and may be withheld without any consequences is clearly valid. Between these two extremes is consent which is more or less conditional upon agreement to some other term or condition. It would not necessarily be unfair that a patient should be asked to consent to the disclosure of data by, for example, a GP to a Health Authority for administrative purposes as a condition of receiving treatment from that GP. By contrast it could be argued that a requirement to consent to the disclosure of data to a medical student as a condition of receipt of treatment in a NHS hospital was unfair.

Thirdly, there must be some indication that the data subject has given his or her consent. This may be express (i.e. explicit) or implied. Express consent is given by a patient agreeing actively, usually orally or in writing, to a particular use or disclosure of information. Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information. For instance a patient who visits a GP for treatment may be taken to imply consent to the GP consulting his or her medical records to assist diagnosis. The Courts have not generally specified whether consent should be express or implied. It is clear, however, that for consent of any sort to be given, there must be some active communication between the parties. It would not be sufficient, for instance, to write to patients to advise them of a new use of their data and to assume that all who had not objected had consented to that new use. It is a mistake to assume that implied consent is a less valid form of consent than express. Both must be equally informed and both reflect the wishes of the patient. The advantage of express consent is that it is less likely to be ambiguous and may thus be preferred when the risk of misunderstanding is greater.
The Commissioner’s approach to medical confidentiality

The Commissioner is not a general source of advice upon confidentiality. However, from time to time, for instance when asked to carry out an assessment of whether the processing of personal data seems likely to meet the requirements of the Act, she must necessarily take a view as to whether firstly, in her opinion, a duty of confidence has arisen and secondly, whether there has been a breach of that duty. Each case must be considered upon its merits. This section of the Guidance describes the general approach.

The Commissioner’s general assumption is that the processing of health data (that is data relating to the physical or mental health of data subjects) by a health professional (see Appendix 2) is subject to a duty of confidence even though explicit consent for processing is not a requirement of Schedule 3 of the Act. This assumption is based upon case law, upon statements made by Ministers at the Department of Health, and upon the advice given by regulatory and representative bodies in the area. The Commissioner distinguishes between a number of broad categories.

As was noted earlier, in some cases, even though data may be subject to a duty of confidence, there may be a justification for disclosure or for secondary use. For instance, the disclosure of information relating to a notifiable disease or a disclosure on the basis of an Order made under s.60 of the Health and Social Care Act cannot be legitimately accused of involving breaches of confidence.

Some other uses and disclosures of data, for instance, routine record keeping, consultation of records etc, in the course of the provision of care and treatment or clinical audit are effectively conditions of receiving treatment. Providing that these uses and disclosures are, as a matter of fact, necessary in order to provide treatment in today’s National Health Service, the Commissioner thinks that it is unlikely that a court would find that consent was invalid by virtue of being made a condition of treatment. Such uses and disclosures may be described as “mandatory” in the sense that acceptance of treatment by the patient will imply consent to these uses or disclosures. (Although it may be generally acceptable to make the giving of consent a condition of treatment, as is discussed in the next chapter, in individual cases where a particular use or disclosure of personal data might cause unwarranted damage or distress, there is a right to object. For instance consent for administrative staff to access medical data for legitimate administrative purposes might generally be a condition of treatment. However, in a particular case, a patient might object if the member of the administrative team was personally known to him or her.)

In most cases where consent is required in order to satisfy the common law duty of confidence, the Commissioner accepts that implied consent is valid. She does not accept that implied consent is a lesser form of consent. Providing that the fair collection information described in Chapter 2 has been provided at an appropriate time, including information as to whether data must be supplied or whether it is optional to do so, and the data subject accepts treatment and does not object to any uses or disclosures of data, then the Commissioner will consider that valid consent has been given. There is an overlap, in other words, between the fair processing requirements of the Act and the consent requirements of the common law.

The Commissioner does, however, think that there are some occasions when express or explicit consent is required. These arise particularly where data have been collected previously without the relevant fair processing information having been provided. This might occur because data were collected before the Act came into force or because the purposes for which it is proposed that data are processed has changed since collection.
In deciding when express rather than implied consent should be obtained and when it is legitimate to make provision of treatment conditional upon agreement to certain uses or disclosures of personal data, the Commissioner will be influenced not only by any relevant case law but also by any Codes of Practice, advice or guidance issued by the Department of Health, NHS Executive, or any of the relevant representative or regulatory bodies. In individual cases she will also take into account any decision or advice given by Caldicott Guardians, or the Health Service Ombudsman.
Chapter 5: The Right to Object to Processing

The Act does not create an overarching requirement that personal data, even sensitive personal data, may only be processed with the consent of data subjects. As was discussed in Chapter 4, however, in many cases it will only be permissible to process health data with the consent of patients not because this is an explicit requirement of the Data Protection Act but because it is a required by the common law duty of confidence and the Act requires that personal data are processed lawfully.

Although data controllers may not be under a duty to obtain patient consent, there are certainly cases where they should give patients the opportunity to object to the processing of their data. There are also cases where data subjects may legitimately object to the processing of their personal data. These issues are considered in this Chapter.

When should an opt-out be given?

The point was made in Chapter 2 that among the other information that should be provided to data subjects in order to make the processing of personal data fair may be information as to whether the proposed uses or disclosures of data are mandatory or optional. The failure to provide this information would be likely to result in personal data being unfairly collected.

In deciding whether to offer an opt-out, data controllers should attempt to distinguish between those uses and disclosures of data which are essential in order to treat patients within the health service and those which are not. By the term “essential” is meant those uses and disclosures without which treatment could not be given and those uses or disclosures which the law makes mandatory. Examples of essential uses and disclosures include:

- Routine record keeping, consultation of records etc, in the course of the provision of care and treatment;
- Processing of records in the event of a medical emergency;
- Clinical audit e.g. the monitoring of a patient care pathway against existing standards and benchmarks;
- Processing for administrative purposes, e.g. disclosure by a GP made in order to receive payment for treatment provided;
- Administrative audit, which may include studies designed to improve the efficiency of the NHS as an organisation, e.g. to support decisions about the allocation of resources;
- Statutory disclosures to disease registries or statutory disclosures for epidemiological research.

In effect these are necessary elements of the medical purpose for which it is proposed that patients’ data are processed. Since it is unlikely to make good administrative sense to offer patients the opportunity to object to the processing of their data for any of the individual elements suggested, it would not make sense to provide an opt-out.

Examples of uses and disclosures that may not be essential include:

- Disclosures to social workers/social services departments;
- Teaching;
- Disclosures to hospital chaplains;
- Clinical trials;
- Disclosures to the media.
In effect these non-essential uses are either for secondary medical purposes, in particular teaching or research, or for non-medical purposes. (Please note: the lists are intended neither to be exhaustive nor to be authoritative. What may be an essential use or disclosure for one data controller may not be essential for another.)

**Opt-outs as means of gaining consent**

In many cases the requirement of the Data Protection Act to provide fair processing information overlaps with the requirement flowing from the common law duty of confidence to obtain consent for the use and disclosure of data.

For instance, patients register for the first time with, say, a cancer clinic. They are provided with standard fair processing information about uses and disclosures of personal data and are also advised that their records will be made available to researchers who may wish to contact them in the future. Any patients who do not object may be deemed to have consented to the disclosure and to being contacted by the researchers.

It is important to distinguish this case, where patients are registering for the first time and thus have not yet provided the clinic with any personal data, from that where the clinic would like to pass the records of former patients to a researcher. On the assumption that patient consent is required (i.e. there is no relevant order under s.60 of the Health and Social Care Act), and that the research exemption is not relevant (since in this case contact by the researcher might cause substantial distress) it would not be sufficient simply to write to former patients giving the opportunity to object. In that case it would be incorrect to infer either consent or an objection from a failure of a patient to respond. The patients would not, in other words, have been given the opportunity to signify consent to the processing of their data.

Where consent to the use or disclosure of personal data is sought after those data were collected, it will normally be necessary to obtain the express or explicit consent of patients.

**The Right to Object to Processing**

An opt-out should be provided wherever patients have a real choice as to how their data are to be processed or wherever this is an appropriate means of gaining consent. In addition, data subjects also have rights to object to the processing of their data whether or not they have been given an opt-out.

Section 10 of the Act sets out the general right to object:

“… an individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstance to cease, or not to begin, processing or processing for a specified purpose or in a specified manner, any personal data of which he is the data subject, on the grounds that, for specified reasons –

(a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or another, and

(b) that damage or distress is or would be unwarranted

Among the important points to note are that objections to processing under this section of the Act must be put in writing, and secondly that the grounds for objection are limited to cases where there is or is likely to be substantial and unwarranted damage or distress to the data subject or
another person. (There will be many cases where it is good practice to act upon an objection made by means other than writing. It would also be good practice to respect an individual’s wishes even if they could not demonstrate that the damage or distress caused to them was substantial.)

A data controller in receipt of a written objection to processing must, within 21 days, inform the person making the objection in writing whether it has complied or intends to comply with the request or must state its grounds for refusing to do so.

The Act gives no comprehensive guidance as to the valid grounds for objecting to the processing of health data, although it makes clear that the interests of the data controller will outweigh those of the person objecting to the processing of data if the processing of data is on the basis of any of the following four Schedule 2 conditions:

- The data subject has given his consent (this condition will be relevant where the person objecting to the processing is a person other than the data subject);
- The processing is necessary for the performance of a contract or for entering into a contract at the request of the data subject;
- The processing is necessary for compliance with legal obligations (for instance a disclosure made on a statutory basis);
- The processing is necessary to protect the vital interests of the data subject (this condition will also only be relevant where the person objecting to the processing is a person other than the data subject).

In the absence of any clearer guidance in the Act, data controllers must judge each objection to processing which is received on its merits. For instance, two individuals may object to their GP to the processing of their data for administrative purposes. In the case of the first, no grounds for the objection are advanced and the GP may be justified in continuing to process the patient’s data for administrative purposes despite the objection (on the assumption that the patient continues to accept treatment). In the second case, a patient objects to the use of data for administrative purposes because a member of the administrative staff in the practice is known to the patient personally and he or she does not wish the details of their medical condition to be disclosed to that person. In this case it is far easier to see that substantial damage or distress might be caused to the patient and it is likely that the GP will decide to make separate administrative arrangements for this patient.

In addition to the general right to object to processing which is, as we have seen, a qualified right, there is an absolute right to object to the use of personal data for direct marketing purposes.
Appendix 1: Practical Application

In this section we seek to apply the analysis of the Principles as discussed in the preceding chapters. Here, the application is limited to those examples listed in the Introduction, but should be sufficiently informative to allow a similar application of the Act to other uses and disclosures of health data.

The tables should not be read in isolation, but in the context of the discussion found in the preceding chapters. Please refer to Chapter 1 for a full description of the use and disclosure headings.

The tables on the following pages are broken down into 4 broad areas:

a) Care and treatment;
b) Administration;
c) Research and teaching;
d) Uses and disclosures for non-health purposes.
# Examples of Uses and Disclosures

**a) Care and treatment**

<table>
<thead>
<tr>
<th>Use or Disclosure</th>
<th>Schedule 2 Condition</th>
<th>Schedule 3 Condition</th>
<th>Fair Processing Information</th>
<th>Lawfulness</th>
<th>PETs</th>
<th>2DPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routine record-keeping; consultation of records etc</td>
<td>Condition 5 or 6</td>
<td>Condition 8</td>
<td>Ensure patient is aware of identity of data controller. Generally assumed patient is aware of these uses and disclosure.</td>
<td>Consent likely to be required to meet Common Law obligations but need not be ‘explicit’ in terms of DPA.</td>
<td>Data must be secure, but there is no general need to use a PET.</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>Processing of records in the event of a medical emergency</td>
<td>Condition 5 or 6</td>
<td>Condition 8</td>
<td>General information should be provided, even though it could be assumed that patients would expect their data to be available in an emergency.</td>
<td>Consent likely to be required to meet Common Law obligations but need not be ‘explicit’ in terms of DPA. If patient was unable to consent, then the public interest may meet the Common Law requirements. Common Law would be breached if it was known that the patient objected to the disclosure.</td>
<td>Data must be secure, but there is no general need to use a PET.</td>
<td>Disclosure is compatible.</td>
</tr>
<tr>
<td>Disclosures made by one health professional or organisation to another</td>
<td>Condition 5 or 6</td>
<td>Condition 8</td>
<td>Only relevant information should be disclosed.</td>
<td>Any disclosures should be explained.</td>
<td>Consent likely to be required to meet Common Law obligations but need not be ‘explicit’ in terms of DPA.</td>
<td>Data must be secure, but there is no general need to use a PET.</td>
</tr>
<tr>
<td>Clinical audit</td>
<td>Condition 5 or 6</td>
<td>Condition 8</td>
<td>Only relevant information should be disclosed.</td>
<td>Any disclosures should be explained.</td>
<td>Consent likely to be required to meet Common Law obligations but need not be ‘explicit’ in terms of DPA.</td>
<td>Strong argument for the use of PETs to protect the identity of patients.</td>
</tr>
</tbody>
</table>
b) Administration

<table>
<thead>
<tr>
<th>Use or Disclosure</th>
<th>Schedule 2 Condition</th>
<th>Schedule 3 Condition</th>
<th>Fair Processing Information</th>
<th>Lawfulness</th>
<th>PETs</th>
<th>2DPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing for administrative purposes</td>
<td>Condition 5 or 6</td>
<td>Condition 8. Only relevant information should be disclosed.</td>
<td>Purposes should be explained in general terms.</td>
<td>Consent likely to be required to meet Common Law obligations but need not be ‘explicit’ in terms of DPA.</td>
<td>Only disclose patient ID if it is intended to contact the patient. Use of PETs is encouraged.</td>
<td>Disclosure is compatible.</td>
</tr>
<tr>
<td>Administrative audit</td>
<td>Condition 5 or 6</td>
<td>Condition 8. Only relevant information should be disclosed.</td>
<td>Uses and disclosures should be explained.</td>
<td>Consent likely to be required to meet Common Law obligations but need not be ‘explicit’ in terms of DPA.</td>
<td>Strong argument for the use of PETs to protect the identity of patients.</td>
<td>Satisfied by a notice given to patients. If not given, it may be possible to rely on S33.</td>
</tr>
</tbody>
</table>
### c) Research and teaching

<table>
<thead>
<tr>
<th>Use or Disclosure</th>
<th>Schedule 2 Condition</th>
<th>Schedule 3 Condition</th>
<th>Fair Processing Information</th>
<th>Lawfulness</th>
<th>PETs</th>
<th>2DPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statutory disclosures to disease registries or statutory disclosures for epidemiological research</td>
<td>Condition 5 or 6</td>
<td>Condition 8. Only relevant information should be disclosed.</td>
<td>Uses and disclosures should be explained.</td>
<td>Common Law obligations met if there is a statutory requirement to disclose e.g. notifiable diseases, or s60 of Health &amp; Social Care Act 2001 (England and Wales only).</td>
<td>Strong argument for the use of PETs to protect the identity of patients.</td>
<td>Satisfied by a notice given to patients. If not given, it may be possible to rely on S33.</td>
</tr>
<tr>
<td>Non-statutory disclosures to disease registries or non-statutory disclosures for epidemiological research</td>
<td>Condition 5 or 6</td>
<td>Condition 8. Only relevant information should be disclosed.</td>
<td>Uses and disclosures should be explained, including that this use of personal data is optional.</td>
<td>Consent likely be required to meet Common Law obligations, but need not be <code>explicit</code> in terms of DPA. Patients have the right to object.</td>
<td>Strong argument for the use of PETs to protect the identity of patients.</td>
<td>Satisfied by a notice given to patients. If not given, it may be possible to rely on S33.</td>
</tr>
<tr>
<td>Clinical trials</td>
<td>Condition 1, 5 or 6</td>
<td>Condition 1 or 8. Only relevant information should be disclosed.</td>
<td>Uses and disclosures should be explained, including that this use of personal data is optional.</td>
<td>Consent required to meet Common Law obligations, and is likely to be <code>explicit</code> in terms of DPA.</td>
<td>Strong argument for the use of PETs to protect the identity of patients.</td>
<td>Satisfied by a notice given to patients. S33 is unlikely to be appropriate.</td>
</tr>
<tr>
<td>Teaching</td>
<td>Condition 1, 5 or 6</td>
<td>Condition 1, 5 or 8. Only relevant information should be disclosed.</td>
<td>Uses and disclosures should be explained, including that this use of personal data is optional, and whether it is hospital or university based teaching.</td>
<td>Consent likely to be required to meet Common Law obligations, but need not be <code>explicit</code> in terms of DPA. Patients have the right to object.</td>
<td>Strong argument for the use of PETs to protect the identity of patients.</td>
<td>Satisfied by a notice given to patients. S33 is unlikely to be appropriate.</td>
</tr>
</tbody>
</table>
d) Uses and disclosures for non-health purposes

<table>
<thead>
<tr>
<th>Use or Disclosure</th>
<th>Schedule 2 Condition</th>
<th>Schedule 3 Condition</th>
<th>Fair Processing Information</th>
<th>Lawfulness</th>
<th>PETs</th>
<th>2DPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosures for Crime and Disorder Act purposes</td>
<td>Condition 5 or 6</td>
<td>Condition 1 or 7. Only relevant information should be disclosed.</td>
<td>Uses and disclosures should be explained, unless prejudicial to S29.</td>
<td>Consent likely to be required to meet Common Law obligations (unless another exception to the duty of confidence applies), but need not be 'explicit' in terms of DPA.</td>
<td>Data must be secure, and anonymised data should be used where possible.</td>
<td>Satisfied by a notice given to patients. If S29 applies, a notice may not be required.</td>
</tr>
<tr>
<td>Disclosures to the police</td>
<td>Condition 5 or 6</td>
<td>Condition 7</td>
<td>Uses and disclosures should be explained, unless prejudicial to S29.</td>
<td>Consent not required if disclosure is in the public interest, or if required by law (e.g. court order).</td>
<td>Data must be secure, but there is no general need to use a PET.</td>
<td>Satisfied by a notice given to patients. If S29 applies, a notice may not be required.</td>
</tr>
<tr>
<td>Disclosures of religious affiliation to Chaplains</td>
<td>Condition 1. Condition 4 may apply in very limited circumstances.</td>
<td>Condition 1. Condition 3 may apply in very limited circumstances.</td>
<td>Uses and disclosures should be explained.</td>
<td>Consent required, unless individual unable to give consent.</td>
<td>Data must be secure, but there is no general need to use a PET.</td>
<td>Satisfied by obtaining consent of patient.</td>
</tr>
<tr>
<td>Disclosures to the media</td>
<td>Condition 1 or 6</td>
<td>Condition 1</td>
<td>Uses and disclosures should be explained.</td>
<td>Consent likely to be required to meet Common Law obligations.</td>
<td>Data must be secure, but there is no general need to use a PET.</td>
<td>Satisfied by obtaining consent of patient.</td>
</tr>
</tbody>
</table>
Appendix 2: Glossary of Terms

Data controller: A person who (either jointly or in common with other persons) determines the purposes for which and the manner in which personal data are, or are to be, processed.

Data subject: An individual who is the subject of personal data.

Health professional: Means any of the following:

a) a registered medical practitioner (a "registered medical practitioner" includes any person who is provisionally registered under section 15 or 21 of the Medical Act 1983 and is engaged in such employment as is mentioned in subsection (3) of that section,)
b) a registered dentist as defined by section 53(1) of the Dentists Act 1984,
c) a registered optician as defined by section 36(1) of the Opticians Act 1989,
d) 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,
e) a registered nurse, midwife or health visitor,
f) a registered osteopath as defined by section 41 of the Osteopaths Act 1993,
g) a registered chiropractor as defined by section 43 of the Chiropractors Act 1994,
h) 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,
i) a clinical psychologist, child psychotherapist or speech therapist,
j) a music therapist employed by a health service body, and
k) a scientist employed by such a body as head of department.

Health record: Any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual.

Personal data: Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller 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 the individual.

Processing: In relation to information or data, processing means obtaining, recording or holding the information or data, or carrying out any operation or set of operations on the information or data.
Appendix 3: Schedule 2 and Schedule 3 Conditions

Schedule 2:

1. The data subject has given their consent to the processing.

2. The processing is necessary -
   a) for the performance of a contract to which the data subject is a party, or
   b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary -
   a) for the administration of justice,
   b) for the exercise of any functions conferred by or under any enactment,
   c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
   d) for the exercise of any other functions of a public nature exercised in the public interest.

6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.
Schedule 3:

1. The data subject has given their explicit consent to the processing of the personal data.

2. The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment. The Secretary of State may by order specify cases where this condition is either excluded altogether or only satisfied upon the satisfaction of further conditions.

3. The processing is necessary –
   a) in order to protect the vital interests of the data subject or another person, in a case where-
      i. consent cannot be given by or on behalf of the data subject, or
      ii. the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing -
   a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade-union purposes and which is not established or conducted for profit,
   b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
   c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes, and
   d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing -
   a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
   b) is necessary for the purpose of obtaining legal advice, or
   c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
7. The processing is necessary -
   a) for the administration of justice,
   b) for the exercise of any functions conferred by or under any enactment, or
   c) for the exercise of any functions of the Crown, a Minister of the Crown or a
government department.

The Secretary of State may by order specify cases where this condition is either excluded
altogether or only satisfied upon the satisfaction of further conditions.

8. The processing is necessary for medical purposes (including the purposes of preventative
medicine, medical diagnosis, medical research, the provision of care and treatment and the
management of healthcare services) and is undertaken by-
   a) a health professional (as defined in the Act), or
   b) a person who owes a duty of confidentiality which is equivalent to that which would
      arise if that person were a health professional.

9. The processing -
   a) is of sensitive personal data consisting of information as to racial or ethnic origin,
   b) is necessary for the purpose of identifying or keeping under review the existence or
      absence of equality of opportunity or treatment between persons of different racial or
      ethnic origins, with a view to enabling such equality to be promoted or maintained, and
   c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

The Secretary of State may by order specify circumstances in which such processing is,
or is not, to be taken to be carried out with appropriate safeguards for the rights and
freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the
Secretary of State.

Data Protection (Processing of Sensitive Personal Data) Order 2000:

Relevant conditions -

7. Processing of medical data or data relating to ethnic origin for monitoring purposes.

9. Processing in the substantial public interest, necessary for the purpose of research whose
object is not to support decisions with respect to any particular data subject otherwise than
with the explicit consent of the data subject and which is unlikely to cause substantial
damage or substantial distress to the data subject or any other person.