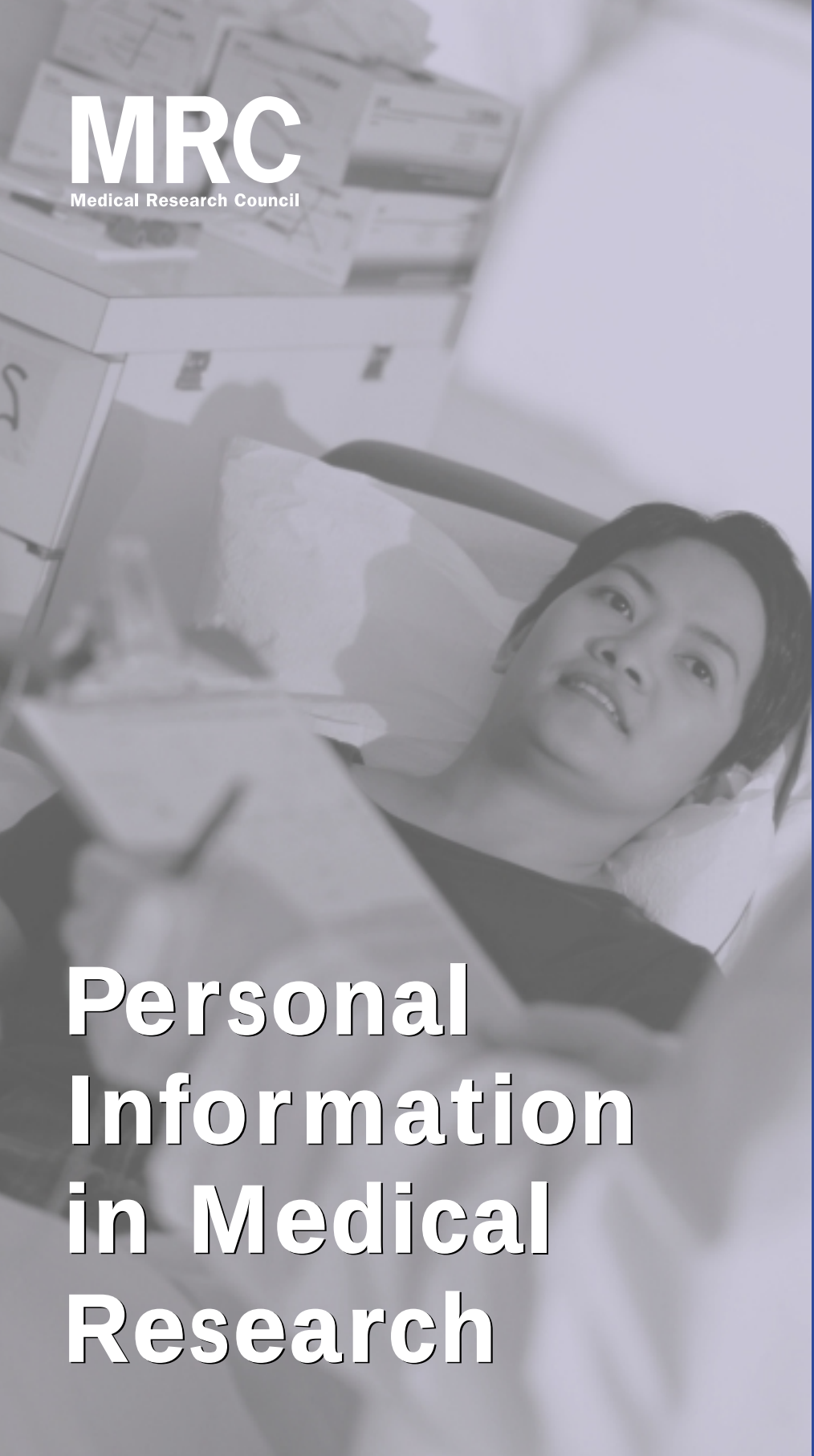


MRC
Medical Research Council

Personal Information in Medical Research

MRC *Ethics* Series

PERSONAL INFORMATION IN MEDICAL RESEARCH

The MRC working group which prepared this guidance comprised:

Professor Andy Haines (Chair, Dept of Primary Care & Population Sciences, Royal Free & University College Medical School)
Dr Richard Ashcroft (University of Bristol / Imperial College School of Medicine)
Dr David Coggon (MRC Environmental Epidemiology Unit)
Dr Angela Coulter (The King's Fund / Picker Institute Europe)
Professor Len Doyal (Queen Mary & Westfield College)
Dr Elaine Gadd (Dept of Health)
Professor Charles Gillis (Dept of Public Health, University of Glasgow)
Dr Naomi Pfeffer (Consumers for Ethics in Research / University of North London)
Professor Michael Wadsworth (MRC National Survey of Health & Development)
Mr Philip Walker (NHS Executive)
Mrs Madeleine Wang (Northern & Yorkshire Multi-Centre Research Ethics Committee)
Professor Simon Wessely (Dept of Psychological Medicine, Institute of Psychiatry)

Office staff
Dr Declan Mulkeen
Dr Imogen Evans
Dr Jenny Baverstock (2000)
Mr Stéphane Goldstein (1999)

Updates to this guidance are available on MRC's website: www.mrc.ac.uk

Copies available from MRC External Communications 020 7636 5422

Contents

Glossary

Personal information, as used in this guide, refers to all information about individuals, living or dead. This includes written and electronic records, opinions, images, recordings, and information obtained from samples. Although anonymised data is not, strictly speaking, personal information, its use is also covered in this guide.

Personal data, in the context of the 1998 Data Protection Act (Section 3.2, and Annex 3), comprise information about living people who can be identified from the data, or from combinations of the data and other information which the person in control of the data has, or is likely to have in future.

Anonymised data are data prepared from personal information, but from which the person cannot be identified by the recipient of the information (see Sections 5.1 - 5.7). The term is used in the guide when referring to linked and unlinked anonymised data together.

- Linked Anonymised data is anonymous to the people who receive and hold it (e.g. a research team), but contains information or codes that would allow others (e.g. those responsible for the individual's care) to identify people from it.
- Unlinked Anonymised data contains no information that could reasonably be used, by anyone, to identify people.

Coded data is identifiable personal information in which the details that could identify people are concealed in a code, but which can be readily decoded by those using it. It is not "anonymised data" (see Section 5.2).

Confidential information is any information obtained by a person on the understanding that they will not disclose it to others, or obtained in circumstances where it is expected that they will not disclose it. The law assumes that whenever people give personal information to health professionals caring for them, it is confidential as long as it remains personally identifiable.

Sensitive information. The term "sensitive" is used in this guide to highlight the need for extra care in using information about mental health, sexuality and other areas where revealing confidential information is especially likely to cause embarrassment or discrimination. Note that "sensitive personal data" is defined in the 1998 Data Protection Act as including all information about physical or mental health or condition, or sexual life (Annex 3(B)).

1 Introduction

Much medical research revolves around information about people - their age, lifestyle, work, and health - drawn from medical records, scientific tests, surveys and interviews. Sometimes, the information also reveals facts about relatives and relationships. These types of information are sensitive and private for many people, although attitudes and expectations vary widely.

Respect for private life is a human right, and the ability to discuss information in confidence with others is rightly valued. Keeping control over facts about one's self can have an important role in a person's sense of security, freedom of action, and self respect. It can also protect against unfair discrimination.

The confidentiality of information patients give to doctors is central to the doctor-patient relationship, and to the public's trust in health care professions. There is little research evidence on how people view the use of this confidential information. The limited evidence available suggests that when asked, the vast majority are willing for information about them to be passed to others, under tight controls, if it will advance medical practice. But many people will not know how information about them might be used, and many others may not even know the sort of information that is contained in their medical records.

Although caution is therefore needed in using any personal medical information, this must be balanced against the potential for improving the quality of care by improving the flows of information within the health care system. At present, compared with what might be achieved:

- information is fragmented, and too difficult to share. It is always difficult to build up a complete picture of the care and treatment people receive - from their GP and in hospital - in order to question whether this could be improved.
- information is often incomplete, and some activities are better documented than others. The results of hospital care tend to be well recorded, while the results of home care or preventive medicine are more difficult to measure and record.
- the information that is available is not analysed fully. Research into the effectiveness of the health services, and into factors affecting the health of people in the UK needs to be strengthened if we are to continue improving the health of the nation.

Medical Research Council staff and grant-holders make widespread use of personal data in clinical research, in clinical trials, epidemiology, and other public health research. In 1972, the MRC set out its views on the conditions under which information about identifiable patients could be obtained and used in research. More detailed guidance was issued in 1985 and 1994. Since 1972, medical research based on records and surveys has led to many important advances in knowledge in the UK, including:

- recognition of new variant CJD and its relation to the BSE epidemic;
- improvements in the organisation and quality of cancer treatment

- better understanding of suspected health hazards - for example, Gulf War related illness and leukaemia in people living near to nuclear facilities;
- reliable evaluations of new preventive measures and treatments - for example, the benefits to people at risk of heart disease from aspirin, warfarin, cholesterol lowering drugs and vitamins;
- ways of reducing cot deaths;
- assessments of the health care needs of special groups in society, such as elderly people;
- identification of adverse drug reactions.

Over the same period, there have been no cases where doctors following these guidelines have been judged in law to have breached confidentiality. But some people involved in research do take exception to the way information about them is used, and many people have strong, general, concerns about the way public and private organisations use personal data.

From time to time, therefore, we have to ask whether the standards that researchers set reflect those society currently expects of us. Many people have a concern that modern information and communication technologies might lead to more casual, or frequent, infringements of privacy. And most people now expect the medical professions, and medical researchers, to be more open and accountable in their work, and to allow individuals more opportunity to be involved in decisions that affect them.

The last few years have also seen active discussion of the implications of the law on data protection for the use of confidential information in research. In 1998, the legal situation changed, with the passing of a new Data Protection Act, and a Human Rights Act guaranteeing respect for citizens' private lives.

Reflecting these changes, this booklet sets out the ethical and legal principles that should now guide the use of personal information in research, and provides a revised code of practice. It supersedes the guidance in the MRC ethics booklet *Responsibility in the use of Personal Medical Information for Research* (1994) and the relevant sections of the booklet *Responsibility in Investigations on Human Participants and Material and on Personal Information* (1992).

The NHS Information Strategy

At the time of writing, work is under way on an ambitious programme of changes in the NHS, including creating lifelong electronic health records for every person in the country, improved sharing and movement of information through an NHS information highway, and more effective use of information to inform NHS management. The strategy creates important opportunities to make some medical research easier and more effective, and to address some of the current concerns around the use of medical information in research. For example, it may become possible to widen the range of anonymised information that is available and useful for research. The strategy will also create new opportunities for health professionals and researchers to engage with members of the public to explain why information sharing is necessary. Researchers need to work with commitment and foresight to make the most of these long-term opportunities. At the same time, it has to be

remembered that information systems designed to support routine health care cannot always be expected to provide the range or quality of information needed for original research.

The status of the guidance
This guidance is primarily for researchers supported by MRC, who are expected to follow it as a condition of funding. The guidance is prescriptive wherever this is appropriate, but like any code of practice, it cannot provide for every possible situation, and exceptions to the general rules will occasionally arise.

We hope that in addition the guidance will be informative and helpful to other researchers, to doctors and other health professionals whose patients' records may be involved in such research, to ethics committees, to others reviewing or supervising research, and to the public.

Scope
This guidance covers all uses of personal information whether or not it is "personal data" under the terms of the Data Protection Act, and whether or not it is confidential (see Glossary). Section 2 summarises the key principles that should guide ethical research, both in general situations, and in situations where research depends on using information without consent. Section 3 outlines the laws relating to confidentiality and personal information, how these relate to ethical principles, and discusses the areas where changes in practice may be needed. Section 4 analyses how the key principles should be applied in situations where consent can, and cannot be obtained. Sections 5, 6 and 7 give detailed advice on good practice, and are relevant to all research using personal information.

The guidance addresses the main uses of this information in medical research, including:

- collection of information as part of clinical trials or other patient-based research;
- use of information from general practice or hospital records to approach people to participate in studies;
- analysing patterns of disease and treatment outcomes from existing records;
- studying the health of people in a particular locality, or with a particular job or lifestyle.

The question of confidentiality often receives most attention in epidemiological or survey work when information is taken from medical records without the person's knowledge or consent, but researchers in every area of clinical and public health research need to respect confidentiality and protect the individual's interests by guarding against accidental or mischievous disclosures, and ensuring the information is not used in ways which could cause distress or harm.

Research use of tissue samples or DNA samples in conjunction with personal data raises special issues since:

- clinical samples, including stored blood, plasma and serum will often be used to answer questions unforeseen at the time they were collected;
- genetic analyses can reveal new

information about an individual, their family members or raise concerns about insurance. Particular care needs to be taken when feeding back information and in the publication of material;
- this information raises special concerns when it is, or is seen as being, predictive of future health;
- some types of genetics research give rise to particular concern - for instance research relating to personality or cognitive function.

Samples, and the information obtained from them, cannot be treated in the same way as other data, and are the subject of separate MRC guidance *Collections of Human Tissue and Biological Samples for use in research.*

Disease registries often provide the starting points for research, and are an essential resource for improving the quality of health services. The NHS Plan[1] published in July 2000 recognises the importance of registries in improving disease management. The House of Commons Science and Technology Committee report "Cancer research - a fresh look"[2] underlined the importance of registries, and the impracticability of only using information in registries with express consent. Because registries are often established for purposes other than research, and because of their diversity, this guidance does not offer detailed advice on good practice. However, we would expect the general principles set out in Section 2 - such as the need to make people aware of how their information may be used - and much of the advice in Sections 5 through 7, to be applicable to research based on disease registries, and to registries maintained solely for research purposes.

Also, while we recognise that it is sometimes difficult to define clear boundaries between research and audit, this guide does not attempt to offer a code of practice for the wide range of activities and situations included in clinical audit. However, we hope that the advice will be helpful to some of those working in audit.

The guidance does not address in detail the question of consent to use information about children, or adults who are incapable of giving consent. Separate MRC ethics booklets give advice on research involving children (1991) and mentally incapacitated adults (1991). The ethical and legal issues in these areas have been actively discussed over the past ten years, and the Scottish Parliament has recently passed the Adults with Incapacity (Scotland) Act (2000), which creates a new framework for consent to research. New guidance will be prepared.

Updates and changes

MRC will keep this guidance under review. The law on confidentiality does not give specific direction on what can and cannot be done in various situations, but some points of law may be clarified in time. In some areas of work, the need for disclosures without consent should decrease with time.

This guide, and all other MRC ethics guides, are available on MRC's website – at www.mrc.ac.uk – and changes will be highlighted there as they arise.

Notes

1 www.nhs.uk/nhsplan

2 House of Commons Science and Technology Committee, Sixth report, Session 1999-2000

2 Principles

2.1 General principles

The following principles should guide all MRC-funded research involving people or their information:

1 Personal information of any sort which is provided for health care, or obtained in medical research, must be regarded as confidential. Wherever possible people should know how information about them is used, and have a say in how it may be used. Research should therefore be designed to allow scope for consent, and normally researchers must ensure they have each person's explicit consent to obtain, hold, and use personal information. In most clinical research this is practicable.

2 All medical research using identifiable personal information, or using anonymised data from the NHS which is not already in the public domain, must be approved by a Research Ethics Committee.[3]

3 All personal information must be coded or anonymised as far as is possible and consistent with the needs of the study, and as early as possible in the data processing. Only personal identifiers that are essential should be held.

4 Each individual entrusted with patient information is personally responsible for their decisions about disclosing it. Health professionals disclosing information should, in particular, ensure they are familiar with the advice of the General Medical Council on disclosures for research. Health care organisations should be aware of the research conducted within the organisation, and should ensure research teams are accountable to them.

5 Researchers must ensure that personal information is handled only by health professionals or staff with an equivalent duty of confidentiality.

6 Principal investigators must take personal responsibility for ensuring (as far as is reasonably practical) that training, procedures, supervision, and data security arrangements are sufficient to prevent unauthorised breaches of confidentiality.

7 Researchers must also have procedures in place to minimise the risk of causing distress to the people they contact in the course of their research. Researchers must also be aware that, despite their best efforts, occasional untoward events may occur and plan for how to deal with these.

8 At the outset, researchers must decide what information about the results should be available to the people involved in the study once it is complete, and agree these plans with the Research Ethics Committee. However, researchers must also be prepared to reconsider if there are unforeseen findings from the study, and discuss the appropriate response with a research ethics committee.

2.2 Information disclosed without consent

2.2.1 Situations arise in which medical research questions can only be answered using personal medical information, but where it is not feasible for those responsible for the individual's care to contact all the relevant people to seek their consent. Based on the ethical and legal advice it has received (Section 3), the Medical Research Council considers that in some circumstances it is justifiable to use personal information, and disclose it to a limited number of other people, without consent.

2.2.2 The principles governing research using information without consent are:

1 Hospitals and practices involved in research must *develop* procedures for making patients aware that their information may sometimes be used for research, and explaining the reasons and safeguards. If patients object to their information being passed to others, patients should have the opportunity to discuss this with their doctor, and their objections must be respected.

2 When consent is impracticable confidential information can only be disclosed without consent only if:

- the likely benefits to society outweigh the implications of the loss of confidentiality, so that it is clearly in the public interest for the research to be done;
- there is no intention to feed information back to the individuals involved or take decisions that affect them, and;
- there are no practicable alternatives of equal effectiveness.

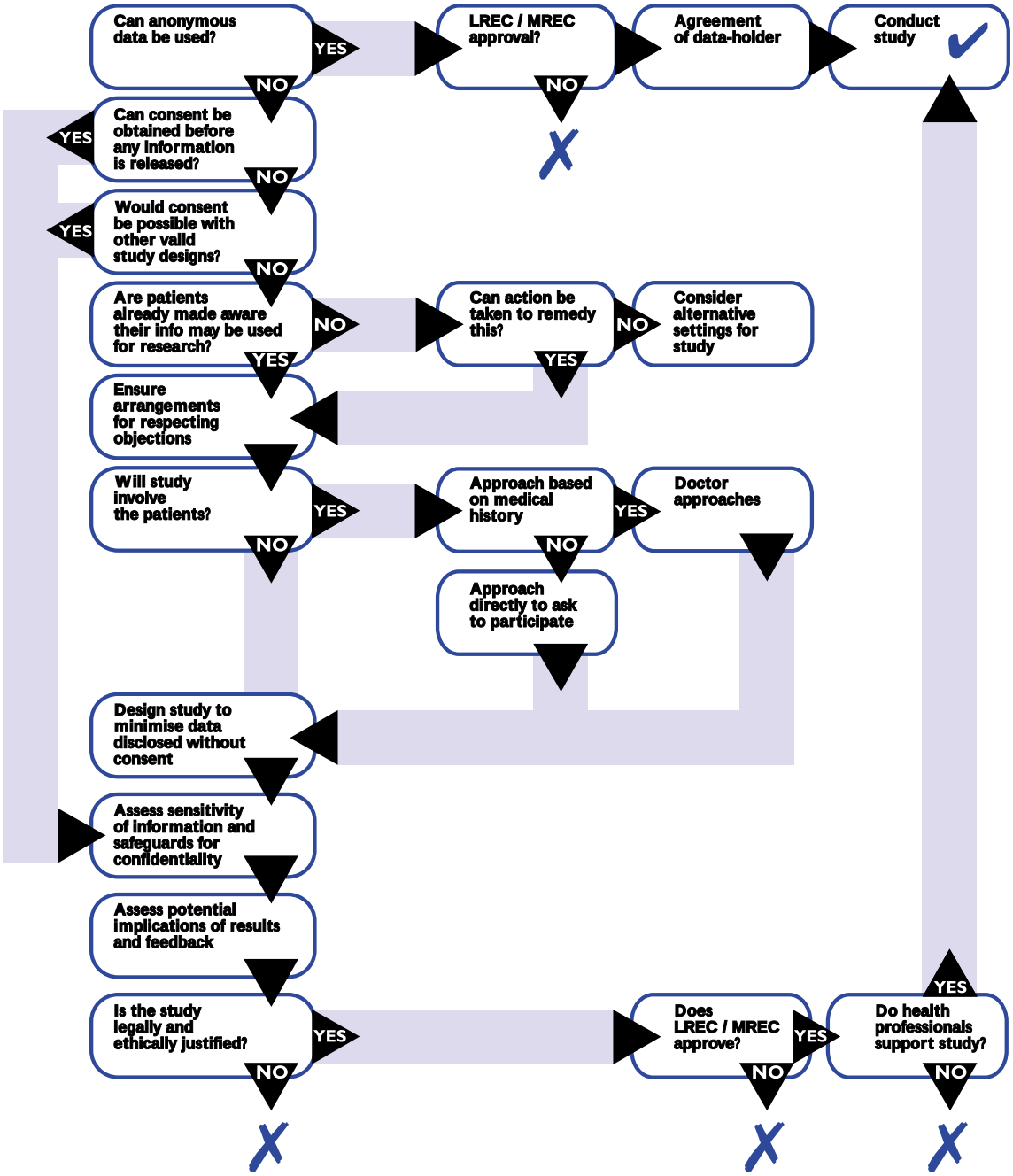
Research must have been planned with confidentiality in mind: from the earliest stages of planning a study, researchers and / or those responsible for patient care should have given careful consideration to whether consent could be made practicable. The judgement that consent is impracticable is never that of the researcher alone: unless an ethics committee concurs, and health professionals agree to participate in the study on this basis, the research cannot take place.

3 The infringement of confidentiality must be kept to a minimum. Even where there is a strong justification for the study, the design must minimise the volume and sensitivity of the personal information that is disclosed, and the number of people who have access to it before it is coded or anonymised. If the disclosure made is to allow researchers to contact people, consent should be obtained then to gather the further information needed, and to hold and process their information.

2.2.3 The diversity of medical research makes it impossible to be prescriptive about the interpretation of these principles. Final decisions on the value *and* acceptability of a

2.3 ***Figure 1 – Using existing personal information in research***

A simplified decision tree



research protocol have to lie with the researchers, the health professionals, and the ethics committee involved, and the organisations which are responsible for supporting and overseeing the work.[4] When considering whether disclosures are justified, one useful aid to thinking might be to ask whether, if the proposed disclosure and the reasons for it became widely known, a reasonable person would see it as unacceptable. A second, narrower test might be to ask whether there are any grounds for supposing that, if consent could be sought effectively, people would be likely to refuse to allow their records to be used.

2.2.4 The conditions in which consent might be practical or impractical, ways of reducing the need for disclosures without consent, and the provision of advance information, are discussed further in sections 3 and 4.

Notes

3 Or, where appropriate, the Scottish Privacy Advisory Committee

4 Principally, the bodies employing researchers, such as MRC, Universities, NHS Trusts

3 The Law as a guide to Good Practice

3.1 Confidentiality in law

3.1.1 In the UK, the confidentiality of personal information is addressed primarily in Common Law. The Data Protection Act 1998 superimposes on this a framework of rights and duties and principles governing the use of information in electronic form or structured paper records. These are discussed below, and Sections 3.3 to 3.6 consider how compliance with the law relates to ethical research practice.

3.1.2 In Common Law, anyone who receives information must respect its confidentiality (that is, not disclose it without consent or other strong justification) if they receive it on the understanding that it is confidential, or in circumstances where there is an implicit expectation that they will not reveal it to anyone else. But while Common Law establishes some core principles, it does not specify when confidential information may or may not be disclosed to others, in research or most other activities. Individuals and organisations using confidential information have to take responsibility for deciding what is justified and acceptable on a case by case basis.

3.1.3 Common Law enshrines the principle that to disclose confidential information about a living person without consent is, generally speaking, to wrong an individual. In law, any information doctors have about their patients must be regarded as confidential, even addresses that might be publicly available elsewhere (for instance, in the electoral register), because the information is given in the expectation that it will not be passed on. Disclosing confidential personal information does not have to cause direct harm or distress for it to be unlawful - any unjustified use of confidential information that weakens trust in the doctor-patient relationship could also be seen as actionable.[5]

3.1.4 However, Common Law also recognises that it can be in the public interest for doctors to disclose confidential personal information, and that the nature and scale of the disclosure has to be balanced against the benefits to society. Interpretations of this balancing judgement vary, and there are few court rulings relevant to the sorts of limited disclosures involved in research. The legal advice to MRC is that the legality of using confidential information in research without consent, could only be judged on a case by case basis, taking into account:

- necessity - were there alternative, practicable, ways of conducting the study, which would have allowed consent to be obtained? Could anonymous data have been used?
- sensitivity - how much did the information reveal about the individual, and was it particularly likely to lead to worry or distress, or damage the doctor-patient relationship?
- importance - was the research well designed, and likely to make a significant contribution to knowledge in the area?
- safeguards - was the amount of information disclosed as small as possible? Were all reasonable steps taken to guard against unintended leaks of information and to maintain trust? Was the risk that the study or its findings might cause distress minimised?
- independent review - was the justification for the research reviewed by a Research Ethics Committee?

- expectations - if explicit consent was not possible, were there reasonable efforts to make people involved aware of how medical records were used, so they had an opportunity to raise any special concerns?

Since anonymised data derived from medical records is no longer information about identifiable people, disclosing it does not breach the duty of confidence to the patient, and these tests do not need to be applied.

3.1.5 Despite the fact that research projects may have been approved by a Research Ethics Committee, and authorised by a Health Authority or Trust, individual doctors remain accountable for their use of their patients' information. The same applies to those who receive confidential information: members of a research team must always be aware that they share a similar duty of confidence to doctors, and that revealing any personal information they hold without good reason - whether resulting from neglect, ignorance, or malice - is potentially actionable.

3.1.6 This is a controversial area of law, and MRC is aware that there are other interpretations of Common Law, some of which would argue for freer use of personal records, and some which hold that the public interest can only justify disclosing confidential information where there is an extraordinary threat to the health of the nation or individuals. MRC has sought to base its guidance on a position that can command broad support, and is consistent with the policies of the Department of Health[6] and General Medical Council.[7]

3.2 The Data Protection Act, the Human Rights Act and other statutory regulations

3.2.1 The UK's 1984 Data Protection Act, and the 1998 Data Protection Act, which replaces it, are both based on the concept of "fair processing". The main principles in the law are explained in Annex 3, but in brief, fair processing means that an individual should normally have the opportunity to know what organisations hold information about them, and why. When people give information, they should be told what it will be used for and to whom it will be passed. They will also be entitled to check records held about them and correct errors.

3.2.2 The Act covers only "personal data", which comprises information about living people who can be identified from the data, or identified from combinations of the data and other information which the person in control of the data is likely to have, either now, or at some future time. Data which have previously been anonymised are outside the scope of the Act.

3.2.3 The law recognises that research needs special freedom to use information in ways not foreseen when it was first collected, and to archive and re-use data. Research work that is not used as a basis for decisions affecting the individuals involved, and which is unlikely to lead to substantial damage or distress, is given special exemptions in these areas (see Annex 3).

3.2.4 The law also sets conditions on when "sensitive personal data", such as information about health, religion, or ethnicity, can be processed. One condition is that the use of the data is necessary for medical purposes, (which are taken to include medical research and the

		TYPE					
		MEDICAL SOURCE				NON-MEDICAL SOURCE	
		Information used in clinical care and research	Information used in research only				
			General personal information	Linked anonymised	Unlinked anonymised	Surveys and questionnaires	Research databases
CONTROLS	Individual controls use of their information	Yes, if able to consent	Where possible	Where possible	No	Yes	No
	Common Law on confidentiality	Yes	Yes	No	No	Yes	Yes
	Data Protection Act applies in full	Yes	If results impact on individuals	If results impact on individuals	No	Yes	No
	Data Protection Act applies with research exemptions	No	Yes, if no significant feedback	Assume yes, if no significant feedback	No	Yes	Yes
	LREC / MREC approval	Yes	Yes	Yes	Yes	Expected*	Expected*

*** MRC expects MREC or LREC approval or equivalent.**

Table 1 – Controls on the use of information in medical research

management of healthcare services), *and* the processing is done by a health professional or a person with an equivalent duty of confidentiality. This condition is in addition to the need to conform to Common Law, and to other sections of the Data Protection Act.

3.2.5 Despite the exemptions mentioned above, the Act is important for research. Fair processing requires that when Health Authorities, hospitals, and doctors know patient information will probably be used for specific research projects, at the time it is collected, they must tell patients this. Health professionals and researchers must give careful thought to whether their use of information might cause substantial damage or distress. Information gathered primarily for research but which will also be used to inform clinical decisions, or which will result in individuals receiving significant new health information about themselves, must comply with every part of the Act.

3.2.6 The Human Rights Act (1998) (Annex 4) established the European Convention on Human Rights as part of UK law. This guarantees the right to respect for private and family life. The body of legal work on the interpretation of this right is still growing, but MRC's legal advice is that, like Common law, it provides for judgements on the balance between the rights of the individual and the legitimate needs of society.

3.2.7 Other relevant statutory regulations are listed and summarised at Annex 5.

Information about dead people, and historical records

3.2.8 The Data Protection Act does not apply to information about a person who is dead before the information is disclosed. Common Law on confidentiality, similarly, is not normally held to apply to information about dead people, although this is a grey area of the law. However, if the use of information about a dead person intruded on the privacy of their relatives - for example, because it revealed information about hereditary conditions or transmissible diseases - then the relatives might be able to take action under Human Rights legislation.

3.2.9 All NHS records are covered by the Public Records Act 1958: GPs' records become public records when they are forwarded to the appropriate local authorities after the death of the patient. While most public records are closed for 30 years, all NHS records relating to a person's physical or mental health are closed for 100 years. The few records kept for long term reference or research are fully open to the public after this point. The Public Records Office will sometimes allow bona fide social, historical or medical researchers access to records within this period, if confidentiality can be guaranteed.

3.3 Ethics and the law

3.3.1 The principles and arguments that underlie ethical reasoning about the use of personal information in research are often broadly consistent with the legal principles discussed above. Interpretations of the law can vary widely, and some interpretations may permit uses of information that are unethical. Therefore, researchers and health professionals should ask first of all whether their actions will reflect ethical and professional codes, and secondly, whether their actions will be consistent with the law.

3.3.2 Over and above legal constraints, there is an ethical imperative not to engage in research which might harm an individual, whether by revealing personal information, or by leading to some intervention in a person's life - such as discovering new facts about their health - that might be against their interests, without their consent. As in all other areas, the presumption should be in favour of allowing individuals themselves to participate in any decision that might affect their interests. Research must not undermine trust in the confidentiality of the doctor-patient relationship, or respect for privacy and confidentiality. Even if it is apparent that a particular use of information cannot embarrass or harm an individual, researchers must ask whether their use of information goes against what a reasonable person might expect, and if so, whether it will, in the short or longer term, erode trust in health professionals or in medical research.

3.3.3 Despite the absence of legal protection, (see above) there is clearly an ethical obligation to continue to respect the confidentiality of medical information after death, and researchers should make sure that disclosures of information are fully justified. Many living people would be distressed by the thought that information about their private lives might be casually revealed after their deaths, especially in the years immediately after their death.

3.3.4 In dealing with disclosures without consent, many international and national ethical codes hold that research based only on records that will not directly affect the individual is one of the few areas where research without explicit consent can be justified. The consensus is that a balancing judgement is needed, setting the risks - often minimal - of harming the individual's interests or undermining respect for confidences more generally, against the likely long-term benefits of the research for society as a whole. However, there has been little emphasis on the need to ask first whether consent is practicable, or advice on how to weigh the different factors in reaching a balancing judgement.

3.3.5 The principles in Section 2, and the remainder of this guidance, draw on both ethical and legal advice.

3.4 Providing advance information about use of medical records

3.4.1 One of the most important steps that can be taken to address the ethical concerns, and to address the legal need for "fair data processing", is to ensure that all NHS patients, are made aware of how records are generally used in research. Explaining what is done, why, and what benefits might accrue, would protect the doctor-patient relationship, improve trust in research, and build realistic expectations of confidentiality. This was advocated by MRC in 1986, and became Department of Health policy in 1996[9], but is not yet widely practised in the Health Service.[10]

3.4.2 It is important, however, that this is not seen as consent to use medical records for any purpose, without either express permission, or proper consideration of the necessity, justification, and potential for harm.

3.4.3 We also have to bear in mind that it will take some time for information leaflets and notices to substantially change awareness of the uses of medical records. Other steps need to be taken, such as asking explicitly for agreement to the use of records in research at an appropriate time, which may be when new patients register with practices, or on first attendance at outpatients, or on admission to hospital.

3.4.4 Providing advance information also raises the question of how to respond when people object to their information being disclosed for research outside of the care team. A request for absolute confidentiality should be discussed with the patient, and has to be respected in all normal situations.[11] If a research study relevant to their health arose in future, their doctor would have to arrange to discuss the study with them and seek their explicit consent before passing on their name: in reality, time pressures would often mean that they would lose the opportunity to participate in the study.

3.4.5 Stated, general objections to disclosure without consent for unspecified studies should not prevent the inclusion of unlinked anonymised information about the patient in aggregated data or statistics (in contrast to the situation where a person declines to consent to a specific study).

3.5 Reducing the need to disclose confidential information

3.5.1 As previously mentioned, the long term development of the NHS Information Strategy will present opportunities to avoid

disclosures of confidential information without consent. Better arrangements for data transfer, standardisation of diagnostic and treatment codes, and improvements in quality control, will gradually make anonymised data from IT systems more useful in research. Public awareness of how medical information is used will also increase.

3.5.2 In the medium term, improving the infrastructure for health services and public health research, especially in primary care, could reduce the need for disclosures, or their scale. Within the MRC's General Practice Research Framework, the presence of research nurses in participating practices means that the preliminary work of selecting patients to receive invitations to participate in clinical trials or surveys can sometimes be done without any information leaving the primary care team until the patient has consented. Where patient details have to be checked centrally before invitations are sent, medical details can often be separated from names and addresses, and codes used to produce standard letters prepared without clerical staff seeing identifiable medical information.

3.5.3 Other primary care networks have, or are developing, similar arrangements and procedures. Researchers should always ask whether their questions can be answered by working only with practices that have the ability to handle information in this way.

3.6 Conclusions and implications for current practice

3.6.1 Clinical and public health research based on, or using, medical records and other personal information is essential if we are to continue to improve public health and health care - in which individuals, as citizens and members of society, have an obvious interest. On the basis of the advice summarised above, the Medical Research Council considers that it should be possible to undertake the full range of research needed in the UK, though some changes in practice are needed.

3.6.2 MRC's advice to health professionals providing information, and to researchers using information, is that they must remain aware that they can be held accountable for their decisions on the use of confidential information. On the question of consent, Common Law does not provide specific answers on when confidential information can and cannot be passed to others without consent, but the advice to MRC has been that use of personal information without explicit prior consent can be legally justified in certain circumstances. Health professionals and doctors must therefore ensure they are familiar with the advice from MRC, the Department of Health, the General Medical Council, and other bodies and should closely follow these guidelines to help ensure that their use of records is ethically and legally defensible, and to minimise the risk of any challenges.

3.6.3 Confidentiality remains a contentious area of law, and MRC cannot *guarantee* that researchers or doctors will *always* be safe from legal challenges by following the guidelines, or because their work has been approved by an Ethics Committee, even though ethics approval is very important. As the General Medical Council advises: "The decision of a research ethics committee would be taken into account by a court if a claim for breach of confidentiality were made, but the court's judgement

would be based on its own assessment of whether the public interest was served."

3.6.4 Current practice varies across the country, but there are 4 areas in which change may be needed:

- patients must, as a matter of course, be given information about how their information may be used, and an opportunity to register and/or discuss their concerns throughout the health service. Where this is not the norm, researchers should press for change;[12]
- researchers have a duty to assess thoroughly, early in the design of a study, whether consent to use personal information is practicable, or could be made so, and to base research on explicit consent where practicable;
- researchers, health professionals and managers need to work together to develop the skills, information technology and infrastructure to facilitate records based research and reduce dependence on disclosures without consent;
- employers need to ensure that all staff using personal information in research have a duty of confidence that is well established through contracts, codes of conduct, and training.

Some of these changes in practice may mean higher research costs: MRC policy has always been to fund its research to the level reasonably needed for the work to be done well, safely, and ethically.

3.6.5 The research team's accountability to the NHS bodies responsible for the patients' care (assuming the researchers are not themselves NHS staff) can be an important safeguard. It is essential for those responsible for research in the NHS bodies involved to be aware of every study conducted, and to be able to call the research team to account if needed. Used as part of an effective research governance framework, honorary NHS contracts can play an important role in strengthening accountability. The Department of Health is currently (Autumn 2000) consulting on proposals for strengthening research governance in the NHS: MRC supports moves to strengthen governance frameworks, and to clarify roles and responsibilities.

3.6.6 *The practicability of consent*

It is difficult to offer detailed advice on when consent is or is not practicable. The most common reasons why consent obtained through the team responsible for a person's healthcare may be impracticable are likely to be the sheer size of the group being surveyed, or the likelihood that many will be uncontactable. However, these obstacles have to be judged in the context of the structure of the relevant parts of the health service: what is impracticable in one setting is not necessarily impracticable everywhere. Other factors may include:

- before a person is asked to participate in a study, someone independent of their doctor, but with the doctor's permission, has to review their records, so that the decision to invite someone to participate is based on specific and uniform criteria;
- excluding people from whom consent cannot be obtained might bias a survey, so that people with a particular background, medical history, or attitude were disproportionately represented. For example, when studying apparent

new health syndromes, or links between treatments and side effects, small or biased samples can give dangerously misleading results.

3.6.7 Very exceptionally, the nature of the research itself may be such that seeking consent, in itself, might cause harm or distress. As a hypothetical example, if a study aimed to examine correlations between parents' mental health and unexplained child deaths, it would be difficult to seek consent without risking causing serious distress. Similar dilemmas may occur in research using tissue samples to generate new information , and these situations are discussed in separate MRC guidance "Collections of Human Tissue and Biological Samples for use in research".

3.6.8 These rare situations call for careful consideration by researchers and ethics committees of where the balance of the patients' interests lies, and of:

- the scope to adopt special consent or counselling procedures that make informed consent achievable. It is important to bear in mind, however, that this standard of informed consent has to be reliably achieved throughout the study if it is to be acceptable.
- the public health importance of the question.
- the likely consequences of eventual publication of the results.

3.6.9 When the risks and the implications of not seeking consent have been fully assessed, the final decisions should be based on whether, despite these risks, it is in the public interest.

Notes

5 That is, a person might have grounds for taking legal action against the person who disclosed it..
6 Health Service Guidance (96) 18 "The Protection and Use of Patient Information". Department of Health, March 1996.
7 "Confidentiality: Protecting and Providing Information", GMC June 2000.
8 See, for example, Canada's Tri-Council Policy Statement *Ethical Conduct for Research Involving Humans* (1998); New Zealand Health Information Privacy Code (1994).
9 Health Service Guidance (96)18 *The Protection and Use of Patient Information.* Department of Health, March 1996.
10 *Report on the Review of Patient-Identifiable Information.* The Caldicott Committee. Department of Health, 1997
11 Exceptions might occur if disclosure could prevent harm or death directly, or address other particularly serious and important problems.
12 Model patient information leaflets or notices will be available from MRC's website in 2001, and a model is available in Health Service Guidance (96)18 *The Protection and Use of Patient Information.*

SCENARIOS
4 Using information with and without consent

Personal medical information is used in almost every type of clinical and public health research, and different research scenarios raise different ethical, practical and legal issues. Outlined below are some of the processes currently used in research. The scenarios are not intended as formulae for good practice, and do not cover every type of research, but are offered as examples for discussing how principles translate into practice, both when consent can be obtained and when it cannot. Whether a particular approach is ethical in a given case will depend on the circumstances of the project.

4.1 Approaching patients during medical care

Scenario A

Patients referred to a specialist centre in a teaching hospital are often involved in the centre's programmes of research on the causes and progression of a disease. Their participation is discussed with them by the consultant when they are first referred. A series of studies by a team of doctors, scientists and technicians draws together information on lifestyle, previous medical history, data from blood samples, X-rays, and CT scans, and information from hospital records about long-term outcomes.

Scenario B

A clinical trial of a new treatment is open to patients presenting in a general practice with defined symptoms. Their GP discusses their participation with them, before passing details to a trials office, to check eligibility and arrange entry in the trial.

4.1.1 In patient-based research involving direct contact with the individual, consent will always be possible, and, therefore, essential. There must be a written record of consent,[13] which includes written permission to use the patient's information in the research, even if it seems a small issue alongside the patient's consent to participate in the research itself, and need not distract from this decision. Patients should also be aware that they have the right to opt out of a study at any time. The main ethical and practical questions, if any, about the use of personal information in

these studies are likely to stem from:

- adequacy of data security and coding / anonymisation and, training and supervision of the group of people who will use the information;
- Longer term storage of the data, or re-use by other groups, or in other research areas.

These are generic questions that have to be addressed in every area, and are discussed in Section 5.

4.1.2 Consent will also be practicable and essential in most prospective studies - for instance, where a health professional takes details from patients knowing that the information will be used for research as well as for normal health care, consent must always be obtained. Researchers should also consider whether it is appropriate to seek permission to use the information again in other studies, and if so, what the patient needs to know about these studies.[14]

4.2 Approaching patients from medical records

Scenario C

Research based on linked anonymised data

To investigate the prevalence of asthma in a population, a study aims to research a cohort of new cases of asthma from a selection of patients from a network of General Practices. The GPs at the practices have already been part of a number of studies and each practice has the support of a part-time research nurse for studies of this kind. The nurse takes personal details of all the patients recorded as suffering from asthma or prescribed relevant medication, and replaces the names with a code before passing details to the research team. The research team identify a sub-set in each practice who should be invited to participate in more detailed studies, and the research nurse approaches them, using letters and information leaflets provided, to seek their consent.

Scenario D

Disclosing names and addresses before consent is obtained

To study the health of an ageing population, a project aims to contact a large sample of the people aged 50-69 in several districts who are registered with local GPs, inviting them to complete a questionnaire and attend their practice for a check up and tests. The general practices consider that they cannot carry out the administrative work of making contact with each person and obtaining consent, even if paid, and instead, they provide the research team with names and addresses. A letter signed by the GP is then sent to each person, explaining the project and asking if they will participate. No other personal information is provided from the GP's records until a person has agreed to participate.

Scenario E

Disclosing information about medical history

To test ways of maintaining the long-term health and quality of life of people with heart disease, a study needs to contact several tens of thousands of potential volunteers, with a

history of angina, heart attacks, bypass surgery or other carefully defined conditions. A team of research nurses identifies people meeting these criteria from a range of different records at dozens of centres, and after checking with the GP, the trials office prepares letters to each individual, on behalf of their GP.

4.2.1 In each of these scenarios, the first question to ask is whether reasonable efforts have been made to make patients aware that their information may be used for research or other purposes not directly connected to their treatment (see Sections 2 and 3.4 above). This might seem unnecessary in Scenario C, which involves no disclosure of confidential information or personal data outside the General Practice, and is unlikely to raise legal or ethical issues other than those mentioned in 4.1.1 above. But even here, steps should be taken to make patients aware that personal information is used in research in the practice, and throughout the NHS, and that the care team includes research staff. In Scenarios D and E, making patients aware of how their information is used is not only ethically important, but would also help to minimise the risk of legal challenge to researchers and health professionals.

4.2.2 Scenarios D and E illustrate the situations that give rise to most ethical and legal uncertainty. Scenario D involves the disclosure of a limited amount of personal information given in confidence without consent, and the justification for this would need to be carefully considered by the health professionals and researchers involved, and by an ethics committee. If patients had previously been given general information about how their records might be used, and opportunity to raise objections, then this very limited disclosure would be unlikely to give rise to any serious objections. If patients had not been given information, then more caution would be needed: there would need to be a clear justification for conducting the research in this setting, and the potential benefits would have to outweigh the breach of confidence involved.

4.2.3 Scenario E involves disclosing information about medical history. While the number of people who have access to the information is strictly limited, the information is undoubtedly confidential and sensitive personal data, with potential to cause some embarrassment or perhaps even discrimination if disclosed. Many other types of medical information, such as information about mental health or sexuality, would be much more sensitive, and more likely to cause distress or embarrassment if disclosed.

4.2.4 If patients were aware of how their records might be used, the researchers, health professionals and ethics committee involved would need to satisfy themselves that the disclosure was necessary and justifiable, and that the information would be used properly (see 4.1.1). The detail of what patients were routinely told about their records, and the degree of sensitivity of the information, would be important factors in the decision.
If patients were not aware that their information might be used in this way, this project would be unacceptable unless there were a strong justification, based on the absence of alternatives and clear potential to benefit health.

4.2.5 The reasons why consent cannot be obtained at the outset differ in Scenarios D and E. In D it is because of the practicality of GPs undertaking large amounts of additional administrative work, in writing letters, chasing and checking replies, and answering queries. In E direct access to medical records is needed to ensure the right people are identified using consistent and objective criteria, which requires appropriately trained and supervised researchers. In both scenarios, the disclosure of identifiable information might be reduced or even avoided if the study could be based in general practices with good facilities for doing research.

4.2.6 The second ethical issue that studies of this sort raise is how to contact people in a way that is unlikely to cause worry or embarrassment. The first approach to people identified from medical records should normally involve a letter signed by the health professional responsible for their care giving information about the research, or accompanied by a letter from the researcher which does so. As well as showing respect for the doctor-patient relationship, this is a vital step in checking that the information on which the researcher acts is up to date, and that those approached are not recently bereaved or likely to be distressed for any other reason. The advice of the person's doctor in this area must always be followed. The same principles apply to approaches based on data from disease registries.

4.2.7 It is acceptable for research teams to provide trained clerical support for the health professional, to prepare and distribute letters and related correspondence, if the clerical staff are bound by a duty of confidence, and the research cannot be in a setting where the care team has the capacity to do this themselves.

4.2.8 The initial letters sent to patients should normally cover all, or some of the following:

- why the research is being carried out, and how participation could help;
- how the patient has been selected;
- that the patient's doctor has considered, and fully supports, the study;
- that there is no obligation to participate, and that their decision will not affect their care;
- what will be involved i.e. in terms of time, interviews, treatment, examinations etc.;
- the benefits (if any) that participants can hope to gain from the research, and whether the study will involve any commitment of time, discomfort, or risk on their part;
- that confidentiality will be safeguarded;
- a contact point in the medical / research team for queries or information. If practical, this would be someone already known to the person;
- a reply form if the patient is willing to give permission without further discussion.

4.2.9 When it is proposed to visit a patient at home, advance notice should be given in the form of a letter from their doctor, explaining the purpose of the procedures, the reason, the name of the investigator, and how they will identify themselves. It must always be made clear that the patient is free to withdraw from the study at any stage. People should normally be given a simple response form with an SAE and adequate time to return it. Providing a Freephone number is also helpful. The care team or researchers should either confirm by telephone, or wait for positive written confirmation that the person is willing to meet

them before calling in person. If the person has previously agreed to take part in the study, and knows a visit will be involved, then it is reasonable to assume that it is acceptable to call at the time suggested unless told otherwise.

4.2.10 Where the study relates to a well defined group, it is usually helpful to publicise the study through newsletters, support groups and similar channels, before, or at the same time as, making direct approaches to individuals. Information needs to be provided in a language that is easy to understand.

Contacting ward patients and patients attending clinics

4.2.11 If the people being contacted are in hospital, or attending a clinic, the patient should be asked first if they will see the researcher, or a member of the care team should introduce the patient to the researcher. Hospitals should also explain, in the information they give to patients, that they may be approached by researchers.

4.3 Research based on existing records and samples only

Scenario F

Stored tissue samples from former cancer patients are to be examined for biochemical markers that might hel predict how the disease will progress, and results will be related to data from medical records on the patient's condition, treatment and outcome. There will be no feedback to the patients, and there is no need to subsequently monitor the longer-term survival of the patients. Thus the data can be anonymised (unlinked) before the analysis, but names have to be used to identify patients and samples when the data are first gathered.

4.3.1 The fact that a study does not require contact with patients is not in itself a reason for not contacting people for consent, if consent is practicable. The justification for this study would need to be considered against the criteria in Section 2, in the same way as (D) and (E) above, though here, the minimal use of identifiable information would be a very important consideration. This type of research also raises the question of when it is right to create new biological information about an individual with or without consent, and these broader issues are dealt with in the MRC ethics booklet "Collections of Human Tissue and Biological Samples for use in research".

Scenario G

Information from hospital records is to be analysed anonymously (unlinked) to identify risk factors predicting poor outcomes from surgery. As the hospital staff cannot be redeployed to extract and anonymise the information, a trained nurse or clerical officer from the research team is assigned to copy and anonymise the information.

4.3.2 Here too, although the justification for the study would still need to be considered by an Ethics Committee, the infringement of confidentiality is minimal, and there are unlikely to be significant ethical or legal objections to this aspect of the study.

4.4 Using information from non-medical sources to contact people

Scenario H

To address concerns about the safety of an industrial process, a research study aims to contact all those who lived in the vicinity of a plant, or who worked there, to survey their long-term health.

4.4.1 Direct approaches to members of the public identified from the electoral roll or other public sources do not require consent or agreement of the individual's doctor, but it is usually advisable to notify local General Practitioners before carrying out a study in an area. MRC expects medical studies of this sort to be reviewed by an LREC or MREC, even though it is not obligatory. Direct postal approaches are generally less likely to lead to distress or misunderstanding than "cold" telephone calls.

Selection by social or disability group

4.4.2 If the research focuses on the health of distinct socio-economic groups (e.g. homeless or disadvantaged people) or people of minority ethnic groups, researchers should consider whether community organisations or other bodies that might be able to represent their interests should be made aware of the study, and should have the opportunity of commenting on the research. When working in areas where there may be significant immigrant populations, and when working with groups with sensory or learning disabilities, researchers should also check whether translators or some other help with communication is needed. It is also possible that some research participants may prefer interviewers of the same gender.

Selection by employment

4.4.3 Occupational surveys to assess risks from work activities, accidents, or from exposure to particular hazards or toxic substances are often based on employers' records. Prior to such a survey, discussions should take place with representatives of the staff involved, with management, the occupational health service, and where possible with the staff themselves. A normal approach would be through a letter confirming that the employer and Trade Union agreed to the study taking place. Publicity through newsletters etc. should also be considered, depending on the sensitivity of the issue being studied.

Notes

13 In a few settings, signed consent is not appropriate, notably in self-administered, anonymous questionnaires – but the uses to which the information will be put must always be made clear to individuals before they fill in the form

14 See Section 8.2

5 Safeguarding confidentiality

5.1 Anonymisation and coding

5.1.1 Information should be modified so that some, or all, of those who might see it are not aware of individual identities, as early as possible in data processing. Although anonymisation may introduce delays and increase risks of error, even a simple coding system provides a safeguard against accidental or mischievous release of confidential information.

5.1.2 It is important to distinguish between the different ways in which personal data can be modified to conceal identities. The definitions we have used in this guide are:

Coded information contains information which could readily identify people, but their identity is concealed by coding, the key to which is held by members of the research team using the information. This might be done, for example, to limit the number of people who had access to information about identifiable individuals, to reduce the risk of accidental disclosure, or when presenting results. This helps to meet legal and ethical obligations to protect personal information, but the research team still holds identifiable personal data, and the use of coded data falls within the scope of the Data Protection Act.

Linked Anonymised Data is anonymous to the research team that holds it, but contains coded information which could be used to identify people. The key to the code might, for example, be held by those responsible for the individual's care, or by the custodians of a larger research database or register.

Unlinked Anonymised Data contains nothing that has reasonable potential to be used by anyone to identify individuals: the link to individuals has been irreversibly broken. As a minimum, unlinked anonymous data must not contain any of the following, or codes for the following:

- name, address, phone / fax. number, e-mail address, full postcode,
- NHS number, any other identifying reference number,
- photograph, or names of relatives.

5.1.3 With both linked and unlinked anonymised data, there is sometimes potential to deduce individuals' identities through combinations of information, either by the people handling research data, or by those who see the published results. The most important potential identifiers are:

- rare disease or treatment, especially if an easily noticed illness/disability is involved;
- partial post-code, or partial address;
- place of treatment or health professional responsible for care;
- rare occupation or place of work;
- combinations of birth date, ethnicity, place of birth, and date of death.

5.1.4 Researchers should always consider - when designing studies, before passing information to others, and before publishing information - whether data contain combinations of such information that might lead to identification of individuals or very small groups. Exactly how much of this potentially identifying information can be safely included in data that is assumed to be "unidentifiable" can only be judged on a case by case basis, taking into account the sample size, the ways in which results will be

published and used, and all other circumstances of the study.

5.1.5 Both types of anonymisation *can help avoid the need to* disclose confidential medical information without consent. Linked data is typically used where it may be necessary to refer back to the original records for further information, or for verification, or if it is planned to provide feedback to patients or those responsible for their care. Unlinked data ensures absolute confidentiality, but by precluding follow-up, verification or feedback, may be incompatible with the research aims, or the interests of the participants and the health service.

5.1.6 If it is practical and reliable, the removal, or coding, of identifying information should be done within the team or organisation responsible for the individual's care. Where this is not possible, it is preferable for a member of the research team to help with the anonymisation rather than for identifiable information be used.

Anonymised data and ethical review

5.1.7 Research Ethics Committee approval is required for the use of coded and anonymised data from NHS medical records. The use of anonymous personal data is much easier to justify ethically and legally, but it must still only be used for bona fide research in the public interest. Removing all apparent personal identifiers will not always protect a patient's identity - for example in cases of rare disease - and anonymous data can still lead to new and disturbing information about groups or districts.

Data in Clinical Studies

5.1.8 In small scale clinical studies, which involve frequent reference by research and medical staff to current patients' conditions, encoding and decoding information can present a significant obstacle to effective team work, and increases the risk of an error that could affect the patient's care. Use of weaker codes (such as initials) in processing research data is acceptable where patients have already given consent to the use of their information in research as well as for their care, and when it can be guaranteed that only a small number of research staff will have access to the information.

5.2 The research team

Members of a research team who use personal medical information should be placed under a duty of confidentiality equivalent to that of a health professional. To reinforce this duty:

- Universities and other research organisations must ensure that all contracts and codes of conduct make clear that any breach of confidence is a grave disciplinary matter;
- team leaders must ensure all staff, students, visiting workers, and collaborators fully understand the standards expected, and the importance of confidentiality;
- team leaders and line managers should ensure that information and advice on principles and practice in this area is readily available.

5.2.1 The Medical Research Council's staff code already creates such an obligation, and it is reinforced by staff training and induction.

5.2.2 As discussed in section 3.6.5, MRC supports moves to clarify responsibilities for research governance in the NHS, and strengthen accountability of researchers to NHS bodies through ensuring better internal information systems and other means.

5.2.3 Access to personal information that is neither anonymised nor coded must be restricted to the smallest number that will allow the study to be done effectively. Access to encoded or anonymised data must also be under the control of the medical director or principal investigator, but the numbers with access can be larger.

5.3 Data Security

Ensuring data are secure is a legal obligation under the Data Protection Act: the level of security, and the cost and effort involved, should reflect the nature of the information and the harm that might result from unauthorised disclosure or loss. Every research team must maintain written procedures for keeping electronic and written personal information secure, which must be enforced and reviewed at regular intervals. The measures needed to protect IT systems and data transfers, in particular, need frequent review and expert local advice should be sought. For this reason, the guidelines that follow should be viewed as a checklist, rather than as a comprehensive guide.

5.3.1 *Responsibilities*

There should be clearly assigned responsibilities for: overall management and control of research data; rapid response to breaches of security or leaks; management of the software; maintenance of backup regime and disaster recovery arrangements; ensuring duplicate files are kept to the minimum needed, controlling access rights, and changing access rights promptly when the team changes. The person or people responsible will normally report directly to the principal investigator on issues of data security.

5.3.2 Responsibilities for data security or disposal at the end of a project (see Section 7) must also be clear. If archived, data must be accorded the same level of security as when they were in active use. If destroyed, all copies of the data must be destroyed in a secure way. Records of destruction must be kept as these may be required for audit or other purposes later.

5.3.3 *Physical Environment*

- Rooms containing paper documents or computers should be accessible only to a limited number of authorised personnel;
- All relevant servers, routers, gateways and other critical equipment should be housed within a secure area;
- Workstations which are logged onto personal research data should not be left unattended;
- Data stored on laptop computers and other mobile machines are always at higher risk of loss or theft. Identifiable personal data should only be stored on these machines in special circumstances – for instance, when patients are interviewed and the data entered directly onto computer. Data thus stored on a laptop computer should then be transferred to a secure computer at the earliest opportunity and wiped from the portable's memory.

5.3.4 *Electronic Environment*

- Access rights to data and applications software should be clearly defined and staff authorised to access personal data should be formally notified in writing of the permissible scope of their access;
- For each application, system users should have a valid user system account name, i.e. a username ID, and a password known only to that user to prevent unauthorised use of systems. Users should be forced by systems to alter their passwords regularly – the frequency may vary according to the constraints of the system software but should be aimed at maintaining high levels of security. Passwords must not be written down or shared with other users under any circumstances. "Temporary" user accounts should not be used;
- A confidentiality warning message should be displayed on entering systems, informing the user that the system contains confidential information and is for authorised users only;
- Users should ensure that, at log-off, documents recently used and containing confidential information are cleared from applications on start up;
- Personal medical information should not normally be sent over the Internet via attached documents, FTP, or other systems. Where this has to be done, the data should be reliably encrypted. Databases transferred by mail should be sent by registered post.

Notes

15 In the accepted information technology sense of the term, overcoming the accidental loss of some or all of the data stored on a system

6 Safeguarding other interests of the individual

6.1 Avoiding harm or distress

6.1.1 Apart from the possibility of allowing personal information to leak out by accident or through deliberate wrong-doing, researchers also need to be alert to the possibility of causing harm or distress through:

- approaching people or families who may be distressed, bereaved, or mentally ill;
- errors in the data used to contact people;
- feeding back findings to study participants and / or families (even where they have requested this);
- publishing findings which could be linked back to participants;
- publishing findings which lead to discrimination;
- allowing re-use of data for other purposes without proper ethical supervision.

6.1.2 The best safeguard against approaching the wrong people, or contacting people who may be distressed by the approach, is the role of the person's doctor in approving the approach, and, where possible, in making the initial approach. However, occasional errors are always possible, and research staff should be prepared to respond to mistakes sensitively and promptly.

6.1.3 The potential for harm to the interests of a defined group may be unavoidable where research has the potential to highlight that group as having, for example, poor health behaviour or being "at risk" from a particular local environmental hazard, or where the research may confirm stereotypes. Researchers must try to anticipate these issues before ethical review, and must consider whether any risk of harm is outweighed by longer term benefits to society, and / or to the group. Researchers must also consider consulting the groups involved, or their representatives, to explain their work, and listen to any concerns.

6.2 Feedback and publication

6.2.1 The question of when study participants should have access to new information specifically about them or their family that is generated in research is dealt with in the parallel MRC guide *Collections of Human Tissue and Biological Samples for use in research.*

6.2.2 The results of clinical trials, records-based research and epidemiological surveys can have substantial implications for individuals. People will be concerned about new risks, or potential side-effects of treatment, to which they may have been exposed, especially if they did not know about the research. Those who have a relevant illness will wonder whether this is as a result of the exposure or treatment. Researchers should liase with Health Authorities, Health Boards, General Practices, relevant consumer organisations or other bodies to ensure people have easy access to good information and advice, before publishing findings which are likely to be contentious or worrying.

6.2.3 The people who have participated in a study should, wherever feasible, be notified of the outcome of the study, and told of the general results. If researchers feel it is impossible or inappropriate to do this, the reasons should be discussed with the ethics committee when approval is sought.

6.2.4 Individuals and families must never be identified in publications without signed consent for that specific publication. Researchers must avoid publishing potential identifiers, such as date of birth or death, which might appear innocuous to the research team but which could reveal the patient's identity to close relatives or friends. Caution is also needed when publishing research about small groups of people, such as work on disease clusters, patient case series in a particular centre, and research on new treatments or rare adverse reactions, especially if the findings are likely to attract a lot of media attention. In these cases there is a particularly high risk that groups and cases may be identified by deduction.

7 Storage and re-use of research data

7.1 Storage

7.1.1 Research records need to be preserved for the longer-term for a number of reasons - other than for historical posterity. Firstly, records may be needed later on for scientific validation of research, or for future research and audit. Secondly, occasionally there is a need for access to records over the whole lifetime of patients, both by the patients themselves (who may have continuing long-term concerns about their own health) and their clinicians – for instance, where trials of novel treatments were involved.

7.1.2 MRC would expect that research records relating to clinical or public health studies should be maintained for twenty years, to allow adequate time for review, reappraisal, or further research, and to allow any concerns about the conduct or consequences of the work to be resolved. Beyond this date, full records may need to be retained for a few studies only, such as those which were of historical importance, where novel clinical interventions were first used, those which have proved controversial, or where research is ongoing. In the remaining clinical and public health studies, and all other studies for which consent was obtained, a subset of the original records, covering the protocol, the consent procedure, the people who consented to take part,[16] and any records of adverse effects should be retained until thirty years have elapsed.

7.1.3 MRC's expectation is that once a research team ceases to exist, when the team leader moves to another centre, or when the team stops working in a particular area, the responsibility for their information passes to the University, Hospital, or research centre. If records are to be stored in the long-term, a custodian must be designated for them, and the custodian's role must include ensuring that information is treated in confidence. If, in due course, the records are to be archived, this should be done in secure repositories. Areas where records may be consulted should be equally secure.

7.2 Re-use of data by third parties

7.2.1 Researchers obtaining information with consent should, wherever possible, anticipate likely needs to archive the data, and to share data sets with other researchers, and make this clear to the people involved. Consent to this should be distinct from consent to the primary use of the information. Existing data sets can be shared with other researchers provided this is not inconsistent with what participants were told about how the data would be used. For example, the use of clinical trial data for meta-analyses should not, in our opinion, require new consent.

7.2.2 In any case where research data are shared with another group for new studies:

- The custodian must ensure that the group accepts a duty of confidence and protects confidentiality through training procedures, etc, to the same standards as the custodian. Normally, only anonymised data should be passed on;
- The custodian must ensure that personal data are not passed to a country without legal protection for personal data equivalent to that in the UK, unless the custodian first assures themselves that the data will be adequately protected in practice. Under the terms of the Data Protection Act 1998, there are no special restrictions on

transfers of identifiable data within the European Economic Area nations.[17] Outside of the EEA - e.g. for data sent to the USA, or any developing country - the custodian must either: remain able to control the use of the data transferred; anonymise the data; or obtain the individuals' explicit consent to send their data to another centre. Further details are available on the WebSite of the Office of the Data Protection Commissioner: www.dataprotection.gov.uk;

- The third party must not pass on the data to any other group;
- Individuals may not be re-contacted except *via* their doctor, or, in the case of cohorts who have given consent, the original research group. Re-contacting individuals involved in past studies requires some sensitivity, as this may cause anxiety and – with the march of time – people may not wish to have a reminder from the past. Re-contacting should therefore only be carried out if it is absolutely necessary, and only with LREC/MREC approval. It should be made clear in the information and consent documents that information from one study may be used in later studies;
- LREC/MREC approval is needed for any use of identifiable data, and for any unidentifiable data taken from NHS records not already in the public domain;
- LREC/MREC approval is not needed for re-use of unidentifiable data obtained directly from study participants, or for re-analysis, by any research group, of unidentifiable data from previous research;
- Where the research group that conducted the study no longer exists, the custodian of the data must ensure that the same standards are applied, and that LREC/MREC approval is obtained where necessary.

Notes

16 Unless the study used anonymised and unlinked information.

17 These are: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden and the UK.

8 Information and consent forms

8.1 Patient leaflets and notices

8.1.1 The Department of Health guidelines *Protection and Use of Patient Information* (1996) provide advice on informing patients and a model notice that can be adapted to suit local needs. Centres active in research will normally wish to include some additional specific information about their research in patient leaflets. This could cover: the reasons for research; the fact that Universities (or other research organisations) work closely with the hospital or practice and regularly receive information; the main sources of funds for the research; that research is independently reviewed; and that all research staff have the same duty of confidence as the health professionals caring for them. Patients should also be told whom to contact if they have any concerns.

8.2 Consent procedures

8.2.1 Where patients are asked to participate in any clinical study, the patient information sheet must directly refer to the treatment of personal data, and explain:

- who will have access to their data;
- the confidentiality of the data (including reference to coding / anonymisation if necessary);
- what will happen to the data once the study is complete.

8.2.2 Where information is being gathered for large scale or long-term studies, such as cohort studies, the information provided may need to include all or some of the following, depending on the nature of the study and the commitment the person is being asked to make:

- the types of studies the records or health data may be used for and the conditions that may be investigated;
- who will be responsible for custodianship of the information (normally this will be the person in charge of the study and/ or the principal investigator) and to what organisation they belong;
- the arrangements for protecting the patient's confidentiality;
- who will have access to the data;
- the uses to which the data will be put;
- whether and how the individual or their doctor will be contacted again;
- the arrangements for actively feeding back information to participants, or providing access to research results;
- (if relevant) that anonymised and unlinked data may be passed on to other researchers;
- that they may ask to see the information held about them and withdraw from the study at any time (if the study design allows data linkage);
- who to contact if they have any concerns about the use of their data;
- what happens to the data once the study is complete;
- how they will find out about any change in the study's direction or custodianship.

8.2.3 If it is expected that data - apart from anonymised and unlinked data - may be used in other, secondary studies, the information may need to explain as well:

- any possible impact of secondary studies on their interests;
- how they can find out about secondary studies;
- what sorts of information might be

passed to others, under what conditions;
- that secondary studies would have to be approved by an ethics committee.

Notes

18 Further advice information and consent forms can be found in the MREC Guidelines for Researchers on Patient Information Sheets

Annex 1
Checklist for records-based research

Context

- Is the study based on a group of patients, or a data set, for which consent has already been obtained?
- Could the study (or parts of it) be done with consent ?
- How well informed are patients in the hospitals / practices about how their information is used? What would they reasonably expect? Have they had an opportunity to express any concerns?

Justification for the study

- How sensitive is the information involved? Are there any particular risks of harm or distress?
- What impact, if any, could the study findings have on the people involved?
- Do the benefits outweigh any foreseeable risks?
- If consent to the study is impracticable, do its potential benefits to people, as individuals or as members of society, outweigh the infringement of confidentiality, and any risks of harm or distress?

Conduct of the study

- If people are being approached, when are they being approached and why?
- If people are being approached, will they get adequate explanation of motives and safeguards, and of their right to opt out. Will it be clear to them that the doctor responsible for their care supports the approach?
- Will the information be anonymised (linked or unlinked) or encoded, and if so at which stage in the project?
- What people will have access to personal information during the study? Have they been made formally aware of their duty of confidence, and suitably trained?
- Do procedures for day to day work, electronic data security, and records storage offer adequate protection for personal information?
- What sorts of findings are likely, and what arrangements are there for these to be fed back to the people involved - if appropriate?
- What will happen to the data after the study is complete?

Annex 2
Responsibilities of a doctor providing personal information

A All health professionals have both a responsibility to protect their patients' confidentiality, and a responsibility for supporting high quality, ethical, research which is likely to benefit their patients as members of the UK public, in the longer term. Health professionals, and especially those involved in research, should ensure that patients are provided with effective information about how medical records are used, and why this is important. This should limit the occasions when responsibilities to patients and to research appear to conflict.

B Health professionals are personally responsible for assuring themselves that their use of confidential information is justified, that practical safeguards to protect confidentiality are in place, and, in particular, that Research Ethics Committee approval has been obtained. They should remember that the ultimate responsibility for protecting their patients' legal rights and *their employer's* interests lies with them, and should ensure they are familiar with guidance from the GMC and other bodies.

C Doctors should normally:

- write a letter to patients when they are first asked to participate in the study;
- ensure they know which patients will be involved, and provide researchers with any advice about patients' circumstances that will help them avoid causing worry or distress. Doctors may sometimes need to advise against approaching a particular individual, without necessarily giving any reason if the reason is itself confidential. This is especially important if the patients will be asked to consent to any physical examination or invasive procedures;
- ensure they are familiar with the design of the study and the safeguards, and able to answer patients' queries, even though the researchers may be the normal contact point for participants;
- when they can do so effectively, and it is consistent with the study design, doctors should anonymise *(linked or unlinked)* the information before passing it on to researchers.

Annex 3 The Data Protection Act 1998

Data Protection Principles

A The 1998 Act, like its predecessor, is based around a set of core 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 subject in relation to the processing of personal data.

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

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

B The "sensitive data" referred to in the first principle includes all information relating to a person's physical or mental health or condition, sexual life, racial or ethnic origin, religious or *political beliefs*, trade union membership, or (alleged) crimes. The references to processing data "fairly and lawfully" draw in the concept of "fair processing" (such as ensuring people are not deceived as to the reasons why information is being collected from them) and also mean that anything which is unlawful under Common Law, cannot be acceptable under the Act.

C Ordinary personal data cannot be processed unless: (The conditions listed below are those most likely to be relevant).

Schedule 2

1 The data subject has given his consent to the processing. *(or)*

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

5 The processing is necessary:
(a) for the administration of justice […]
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person. *(or)*

6 (1) 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 by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
(2) The Secretary of Sate may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Schedule 3

In addition, sensitive data cannot be processed unless:

1 The data subject has given his explicit consent to the processing of the personal data. *(or)*

8 (1) The processing is necessary for medical purposes and is undertaken by :
(a) a health professional, or
(b) a personal who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
(2) In this paragraph "medical purposes" includes the purposes of preventive medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

D Use of data for medical research will normally be justifiable under Sections (1) or (6) of Schedule 2, and Sections (1) or (8) of Schedule 3. However, the fact that use of medical records is acceptable under these clauses of the Act does not necessarily mean it is lawful or fair: it also to be consistent with Common Law on confidentiality, and with general concepts of fairness.

E The Act recognises that research work and statistical work often require information to be processed

in ways other than those for which it was collected, and that it is often unreasonable to expect members of the public to know about this processing, or to have the right to access the data. Research is given special exemptions in Section 33 of the Act.

Research, history and statistics

33(1) In this section, "research purposes" includes statistical or historical purposes; "the relevant conditions" in relation to any processing of personal data means the conditions:
(a) that the data are not processed to support measures or decisions with respect to particular individuals, and
(b) that the data are not processed in such a way that that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

33(2) For the purposes of the second data protection principle, the further processing of personal data only for research purposes in compliance with the relevant conditions, is not to be regarded as incompatible with the purposes for which they are obtained.

33(3) Personal data which are processed only for research purposes are exempt may, notwithstanding the fifth data protection principle, be kept indefinitely.

33(4) Personal data which are processed only for research purposes are exempt from section 7 if -
(a) they are processed in compliance with the relevant conditions, and
(b) the published results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

(Note: Section 7 of the Act deals with individuals' right to access the data that organisations hold on them)

33(5) For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed:
(a) to any person, for research purposes only
(b) to the data subject or a person acting on his behalf
(c) at the request, or with the consent, of the data subject or a person acting on his behalf
(d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b), or (c).

Annex 4 The 1998 Human Rights Act

The 1998 Act incorporates the rights and freedoms set out in the 1950 European Convention on Human Rights into UK law. The Act gives UK courts the authority to rule that existing or new UK laws are incompatible with these rights and freedoms. The Act makes it unlawful for a public authority, by its acts or failures to act, to conduct itself in a manner incompatible with the Convention. Courts can hear cases brought by people affected by the actions or inaction of public bodies, and can order public bodies to make redress or pay damages.

The interpretation of the Act in the UK will take account of previous rulings by the European Court of Human Rights.

The Convention covers matters such as:

- protection of property
- the right to life
- prohibition of torture
- prohibition of slavery and forced labour
- right to liberty and security
- right to a fair trial
- prohibition of punishments without legal foundation
- right to respect for private and family life
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly and association
- the right to marry

The Act sets out situations in which laws can restrict these rights, for example to prevent civil disturbance or protect public health, and possible justifications for public bodies infringing these rights. In relation to the right to respect for private and family life, the Act states:

1 Everyone has the right to respect for his private and family life, his home, and his correspondence.
2 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.

The confidentiality of medical information about a person is seen as an integral part of respect for privatand family life. Previous European cases dealing with disclosures of medical information in criminal cases and other areas have focussed on:

- whether the disclosure was in accordance with national law
- whether it was necessary
- whether it was proportionate (i.e. no greater than needed for the purpose).

Annex 5 Other statutory requirements

Aside from the Data Protection Act 1998, there are other statutes and regulations on the disclosure of information:

- The NHS (Venereal Diseases) Regulations 1974 and the NHS Trusts (Venereal Diseases) Directions 1991, prevent the disclosure of any identifying information about a patient examined or treated for a sexually transmitted disease (including HIV and AIDS) other than to a medical practitioner (or to a person employed under the direction of a medical practitioner) in connection with and for the purpose of either the treatment of the patient and/or the prevention of the spread of the disease.
- The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992, limits the circumstances in which information may be disclosed by centres licensed under the Act.
- The Abortion Regulations 1991 impose obligations on medical practitioners who carry out terminations of pregnancy to notify the Chief Medical Officer and to provide detailed information about the patient. The Chief Medical Officer may then only disclose that information in accordance with the provisions of the regulations.

Source: 'For the Record: managing records in NHS Trusts and Health Authorities', *Health Service Circular HSC 1999/053 (March 1999).*

Other publications in this series

The Ethical Conduct of Research on Children, December 1991 (reprinted 1993).

Responsibility in the use of Animals in Medical Research, July 1993.

Responsibility in the use of Personal Medical Information for Research – Principles and Guide to Practice, Prepared for Council's standing Committee on the Use of Medical Information for research, 1985. Reprinted with minor revisions as footnotes, September 1994. To be revised 2001.

Principles in the Assessment of Medical Research and Publicising results, January 1995.

MRC policy and procedure for inquiring into allegations of scientific misconduct, December 1997.

The Ethical Conduct of Research on the Mentally Incapacitated, December 1991Reprinted August 1993.

Collections of Human Tissue and Biological Samples for Use in Human Research. Available January 2001.

MRC

Medical Research Council

20 Park Crescent, London W1B 1AL

Telephone: 020 7636 5422 Facsimile: 020 7436 6179

Website: www.mrc.ac.uk