ABPI GUIDELINES FOR THE SECONDARY USE OF DATA FOR MEDICAL RESEARCH PURPOSES

The Association of the
British Pharmaceutical Industry
12 Whitehall London SW1A 2DY
Telephone: 0870 890 4333
Fax: 020 7747 1411
E-mail: abpi@abpi.org.uk
Web: www.abpi.org.uk

ABPI GUIDELINES FOR THE SECONDARY USE OF DATA FOR MEDICAL RESEARCH PURPOSES

The Association of the
British Pharmaceutical Industry
12 Whitehall London SW1A 2DY
Telephone: 0870 890 4333
Fax: 020 7747 1411
E-mail: abpi@abpi.org.uk
Web: www.abpi.org.uk

CONTENTS

FOREWORD BY THE INFORMATION COMMISSIONER

People have always considered information about their health to be particularly private. They want it to be kept secure and only used for proper purposes. The ancient origins of the health professional's duty of confidentiality reflect this. However, individuals also want medicines that are effective against the ailments that trouble them. In order to develop these medicines researchers need access to information about people. So, we have a potential tension: the desire for privacy on the one hand, the need for access to information on the other.

The effect of data protection law on medical research has often been a contentious and misunderstood area. However, data protection law provides an effective framework for managing the tension between privacy and access to information. This guidance will help medical researchers to make the best use of personal information whilst respecting the people it is about. Its emphasis on consent and transparency is particularly welcome.

Medical researchers' adoption of best practice in the handling of personal information will engender the trust of the public and encourage their participation. Ultimately, it will help to deliver the obvious benefits that medical research can bring.

Richard Thomas

Information Commissioner

EXECUTIVE SUMMARY

The discovery and development of medicines requires the use of individuals' medical information - for example in the conduct of clinical trials to evaluate the efficacy and safety of an investigational medicine. This information is collected and used according to ICH GCP which requires informed consent, ethics committee approval and other measures such as removing information that can directly identify the individual and coding the data to protect patients' privacy and confidentiality.

Medical information used in research cannot be used by researchers to directly identify individuals except where regulation allows. Furthermore, where individuals' medical information is used for additional or secondary research, additional measures are put in place to protect the privacy and confidentiality of individuals. These include re-consent or anonymisation of the information. This ABPI document provides guidance to Member Companies on appropriate measures and considerations when using individuals' medical information for additional or secondary research uses.

PART 1: BACKGROUND AND LEGAL FRAMEWORK

SECTION 1: Introduction

The role of the pharmaceutical industry is to invent, develop and deliver medicines which can be used to prevent or treat illness and disease and to monitor the efficacy and safety of those medicines. The development of medicines and the study of their efficacy and safety is a lengthy and detailed activity which involves considerable data input based on individuals and their experiences to ensure that appropriate medicines are produced which are as safe and as effective as possible.

Medical data, including personal information, which are gathered and processed during the course of inventing, developing and delivering a particular medicine may be a valuable source of information in work carried out to invent, develop and deliver other future medicines. The purpose of this Guidance is to set out the type of data which are typically and essentially part of the process of bringing new medicines to market and to provide guidance on how such data may be acquired and used beyond the original purpose for which the data were collected. The ABPI is aware of, and sensitive to, concerns about data privacy. Its intention in promulgating this Guidance is to set an effective standard which safeguards the legal and ethical needs of the community, whilst affording the pharmaceutical industry an appropriate opportunity to deliver medicines which benefit society. Whilst this Guidance is voluntary, ABPI hopes that its member organisations and others will wish to adopt its provisions.

The gathering and use of personal data is governed in the United Kingdom by the Data Protection Act 1998 and subordinate legislation. This in turn stems from the European Council and Parliament Directive 95/46/EC. The purpose of that legislation is to afford rights to individuals and to assure them that information which is held about them, and from which they can be identified, may only be gathered and used if certain stipulated conditions are met.

The ABPI fully supports the provisions of, and the principles behind, the Data Protection Act 1998.

Pharmaceutical companies are keenly aware of the need to protect personal data. Individually and collectively they adopt a number of measures to ensure that legal requirements are observed and that individuals can rest assured about the treatment of their personal data. These measures vary and include, but are not limited to, the appointment of specialist data privacy officers; the development of Standard Operating Procedures to be observed by company staff for the collection and treatment of personal data; and the regular training and development of staff involved in this field.

Medical data can arise in many contexts, including:

- the running of 'healthy volunteer' studies when the physical effects of a medicine are studied in volunteers in good health
- the running of clinical trials for new medicines with a wider range of volunteer patients who suffer from the disease to be treated
- post marketing studies
- clinical trials for the new use of an existing medicine
- off-label prescription
- adverse event reporting
- prescription data

Pharmaceutical companies may wish to use information gathered under the above scenarios as part of the process of developing and obtaining approval for new medicines and/or in making information publicly available concerning developments in a particular medicinal field.

This Guidance will analyse the type of medical data which might be put to a secondary use (i.e. a use which is secondary to the primary purpose for which the information was originally obtained). It will explain what type of information may be gathered and processed in line with the Data Protection Act 1998 and other UK laws. In addition it will describe what consents must be obtained or other processes gone through if that information is to be considered lawfully gathered and capable of being processed for a further use.

This Guidance is commended to all organisations engaged in the secondary use of medical data for research purposes and will provide the balance between much-needed information which is critical in the development of medicines for the public good and the need to protect the public from collection of

personal information which is intrusive and beyond the need of companies in that role. Please note that the Guidance is just that and is not intended as a substitute for legal advice.

Please see Section X for definitions of various terms.

SECTION II: Scope and Aim of this Guidance

1. SCOPE

- This Guidance only applies to medical data that are processed in the UK. If the transaction involves a foreign element, you should seek legal advice to ascertain whether the proposed processing is subject to the UK Data Protection Act 1998 and/or is subject to foreign legislation. Circumstances in which to seek advice might include, for example, if the data are generated abroad; or the data processor is based abroad; or the data controller is not UK-based. See Section 5 of the Data Protection Act 1998
- The Guidance applies to the secondary use of medical data in its widest sense and regardless of its original source but including that generated within the NHS or already held by companies as part of their previous clinical trial activities. This would include, for example, treatment data, adverse drug reaction data and disease registers
- If any medical data identifies a living individual then the Data Protection Act 1998 applies
- If medical data are anonymised then, by definition, individuals are not identifiable and the Data Protection Act 1998 does not apply

2. AIMS

The aims of this Guidance are:

- Primarily to protect individuals whose personal information is being analysed and secondarily to inform the company making use of such data
- To provide guidance on what steps to take to enable the secondary use of medical data, including anonymisation
- To clarify the legal requirements in one of the most frequently encountered situations, namely the use of coded data derived from clinical trials where the key code holder is legally separate from the person receiving the data for analysis and the recipient cannot readily identify the individual from the data
- To enable the continuation of research with the secondary use of medical data with appropriate safeguards

SECTION III: The Legal Framework

Go to Appendix I for a full explanation of the legal background.

PART 2: PRACTICAL CONSIDERATIONS

Having referred you to the legal framework (Appendix 1) relating to secondary use of data, the following sections are designed to bring a number of practical considerations to the fore and explain some useful steps which a data controller might consider in order to maximise the likelihood of being able to use such data.

The decision tree set out in Diagram 1 shows the key questions to ask.

The following sections address the issues in further detail.

SECTION IV: Checking Sources of Primary Data

Data researchers are advised to review the data they wish to use for secondary research. In particular, when considering the secondary use of data, researchers are advised to take the following steps:

1. Prepare an inventory of candidate sources. Sources could include:
   - Databases from clinical trials
   - Databases from epidemiological studies
   - Data gathered from routine healthcare
   - Safety data reporting
   - Data from service providers

2. Review the extent of anonymisation/codification already applied to the data and perform risk assessment for identifiability of subjects. Pay particular attention to potential identifiers in place, including the presence of rare disorders, and, in the case of key coded data, who holds the key and on what basis

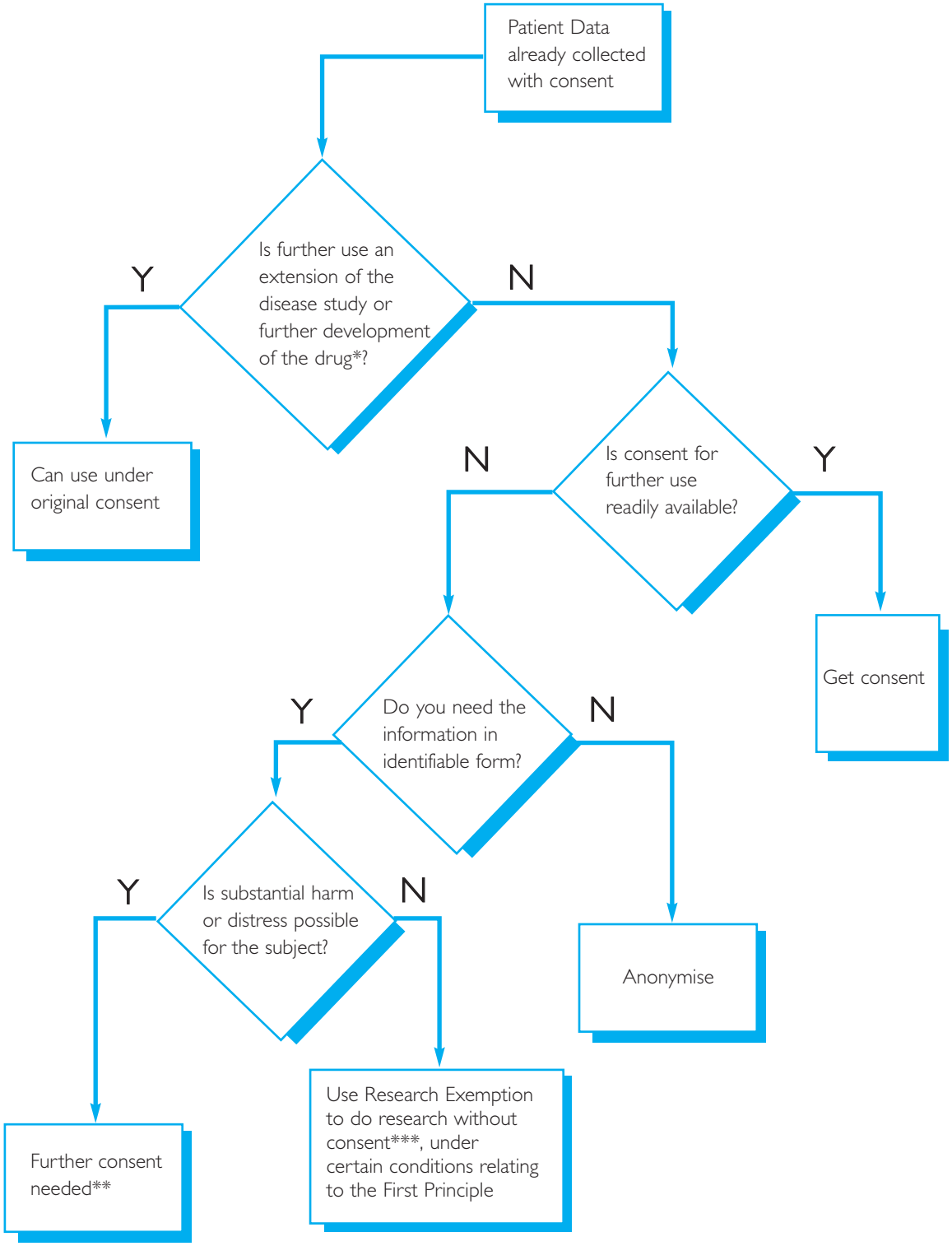
3. Review the nature and scope of any information provided to data subjects and consents supplied to them when the data were gathered for the primary purpose (including fair processing notices)
   - Are there any statements concerning potential future uses of data?
   - Are there any statements concerning the planned duration or storage of the data?
   - Is the current proposal compatible with the original consent, and thus not truly secondary use?

4. Generate a risk statement summarising the proposal and including:
   - Evaluation of the likelihood of being able to identify individuals from the datasets involved
   - Compatibility with the original stated purpose for gathering the data
   - Justification for the proposed secondary use of the data

5. Once this exercise is completed then it should be possible to determine:
   - if tracking down and re-consenting the data subjects is needed, or
   - if the data should be anonymised, or
   - if other provisions of the DPA or Health and Social Care Act 2001 enable processing for a secondary use

in order for that information to be considered lawfully gathered and capable of being processed for a secondary use.

DIAGRAM 1: ABPI GUIDANCE - SECONDARY PROCESSING



* If further development is inconsistent with the original consent, then original consent cannot be used.
** Or seek PIAG approval via Section 60 of the Health and Social Care Act 2001.
*** Common Law would also require there was an overriding public interest in doing the research.

SECTION V: Advance Planning to Maximise Use of Data

When medical data are first obtained, the type of data to be collected and the purposes for which those data will be used are usually provided. In a clinical trial scenario these would be defined in both the clinical trial protocol and the patient information sheet/informed consent form.

However, less thought is usually given to further analyses/processing which it may be desirable to carry out on these data at a later point in time.

The ease with which secondary processing can occur can be significantly increased if:

- The data collected are anonymised prior to secondary processing so that the need to obtain consent is removed
- Any trial protocol contains an outline of any secondary processing which may need to be carried out should the data collected as part of the primary data processing activity indicate the need to conduct further analyses. Whilst these needs are difficult to predict at the start of a study, on-going discussions with health authorities and experts should enable these needs to be more proactively identified
- Any patient information sheet /informed consent form contains wording which informs the patient that further analysis may be required (at a later date) of the data already collected on them in order to support further development of the drug, future drugs and/or greater disease understanding or because of requests from health authorities to provide further data on patients who have taken the drug in previous trials. Assurance that patients' confidentiality will be maintained, insofar as the law allows or permits, should also be given
- Assurance is given to patients regarding security measures that will be taken to protect their personal data

SECTION VI Secondary Use of Data

In general terms, acceptable further use of primary data for secondary processing without resorting to re-consent would include additional analysis within the scope of the original consent for the further development of the drug at the same time ensuring that no harm or distress would come to the individual.

Testing hypotheses or carrying out studies outside of the original consent, would require re-consent (or anonymisation) or other provisions of the Data Protection Act 1998 or the Health and Social Care Act 2001 as described in detail below.

1. Possession of the data

To process the data, the data controller must have legitimate possession of it, for example, he must already be using the data legitimately in primary research, normally by way of informed consent.

For data bought in from an external source e.g. a university or third party organisation, (including gifting from external sources), some evidence of transaction e.g. a contract, notification of gift etc will be needed to show that the data controller has a right to the information.

2. Do I have consent to use this data for secondary purposes?

If within the bounds of primary consent as described above, then yes.

If outside the bounds of the primary consent, then no.

If the data are bought in or received in some other way, the original consent needs to be examined to determine the scope of the consent that was originally given. Depending on the existence / extent of the original consent, re-consent, anonymisation or other processes may need to be gone through if that information is to be considered lawfully gathered and capable of being processed for a secondary use.

The following may be helpful considerations when drafting consent forms to ensure the maximum utility of the personal data collected. State explicitly that:

- personal data will be collected for legitimate, identified purposes, in addition to the collection of any physical samples as required
- The personal data collected will be processed by computer e.g. analysed, aggregated etc
- the patients' information benefits from the protections of a key-code and that only the investigator can unlock that code in accordance with the protocol. Only in specific and limited circumstances is the sponsor of the clinical trial given personal (as opposed to coded) data

- the personal data will be transferred to countries outside of the EEA. Where possible name these countries. Irrespective of destination, stress that the personal data will always be handled to the same standards imposed by English law and GCP (unless local law dictates otherwise)
- the patient may withdraw (or be withdrawn) from the clinical trial, in which case no further samples and/or personal data will be collected from or about them
- their rights of subject access may be curtailed to the extent that the data remains key-coded

3. Options if original consent cannot be used :

- obtain re-consent
- anonymise the data (see anonymisation section below)
- if it is not practicable to locate a patient to re-obtain consent without unreasonable effort and the likelihood of detriment to the patient is negligible, use of previously collected data for research purposes may be justified based on the research exemption (Section 33 of the Data Protection Act 1998). Further details about this exemption are set out in Section III under the heading of the Second Data Protection Principle. Whilst not, strictly speaking, a data privacy issue, have some regard for whether it is appropriate to contact persons a long time after a trial has concluded. This may be particularly relevant in sensitive areas such ascancer or fertility research
- for other data uses, it may be appropriate to apply to the Patient Information Advisory Group (PIAG) under Section 60 of the Health and Social Care Act 2001 for dispensation to proceed without consent (this process applies only in England and Wales and requires several approval stages). Further details are set out in the diagram.

For options where consent is not available, it would be prudent to record the justification for choosing one of the options above. This may document situations where disproportionate effort would be involved in seeking consent.

Not withstanding the above, the MRC recommend Ethics Committee approval for all studies funded by them, even if using anonymised data. One of their principles focuses on NHS data but may be applied more widely: *"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".*

4. Withdrawal of consent by patient

This may occur either during primary or secondary processing:

- data already collected needs to be preserved for clinical safety reasons but no more data can be collected other than that defined in the protocol and consent
- any access to the data by the individual, as permitted by law, will be delayed until the study is completed to ensure the integrity of the study. In addition, any access to data would need to be via the investigator who holds the coding key
- any samples collected will not be used for secondary research purposes unless stated in the protocol and within consent or anonymised

5. Use of Coded Data

Coded clinical trial data (**see Section X: Definition of "Coded"**) is not anonymised since a decode listing exists and it is therefore possible for the patient, under certain circumstances, to be identified by the key-holder. However, the data is heavily protected by a secure key code in the control of the investigator and access by anyone else is not permitted, except where the law allows. Because the key code is not in the possession of, or likely to come into the possession of, anyone who is not the investigator, it cannot be used to identify an individual.

Secondary use of coded data by the **key-holder** is required to meet the authorisation options described in the above subsections. Secondary use by those who **do not have access** to the key code, or are unlikely to have access to it, e.g. the clinical trial sponsor, will not, in theory, be required to meet one of the authorisation options when operating solely within the UK. In practice however where clinical trial data are generated from international multi-centre studies, the UK specific authorisation processes will not facilitate secondary use of data from all sites and anonymisation may be the appropriate course of action.

6. Detailed consideration of anonymisation

Anonymisation of data **(see the definition of "Anonymised" in Section X)** can be achieved by ensuring any link between the data and the individual has been severed and sufficient identifiers have been removed to protect an individual's privacy. However, removal of some identifiers does not necessarily lead to anonymisation. Industry standards have yet to be set, but an acceptable level ofanonymisation can be achieved which gives protection to the individual and at the same time allows research to be conducted. This acceptable level of anonymisation involves the removal of the obvious identifiers e.g. name, address, social security number or such like, so that there is little likelihood of theindividual being identified. Thus, an individual's medical data can be collected and collated for research purposes with little likelihood of the identification of the individual themselves.

An example of anonymisation is a medical research database where the following identifiers are removed: patient name, patient code number, patient address, social security number, NHS number, subject initials and where possible date of birth (in the latter case if age can be used then it should). This will give in normal circumstances a reasonable expectation of anonymisation.

It is of note that removal of **all** of the identifiers as in the Privacy Rule of the US Health Insurance and Portability Accountability Act 1996 where all 18 identifiers need to be removed to attain de-identification extensively curtailed research, in the process raising the protection of the individual to an excessive and unnecessary level. A compromise was introduced called a *limited set* where geographic area codes and hospital dates of entry and departure were retained allowing certain types of research e.g. epidemiology studies to continue under a data agreement.

Anonymisation can also be greatly assisted by technology, particularly encryption technology which can afford additional safeguards.

EXAMPLES OF ANONYMISATION

7. Following on from the discussions above, where anonymisation is required, an acceptable level of anonymisation can be derived as follows

DATA TYPE	IDENTIFIERS TO BE REMOVED TO MAKE THE INFORMATION ACCEPTABLY ANONYMISED
Medical research database holding coded study data	Subject name Code or subject number Address Social security number Hospital number Subject initials
Clinical database holding clinical trial study data where the data are single or double coded (and does not contain identifiers such as subject name, code number, address, social security number, hospital number or subject initials). Double coded data has an additional privacy safeguard imposed by the use of a second coding system. Adding an additional code to the data provides further protection. The investigator holding the first code does not have access to the second code	The link between the individual and the data is severed. When the key codes are destroyed, the data has no link to the identity of the individual and hence the data can be considered to be anonymised.
Samples Collection: Bought-in samples from a third party e.g. a university	Subject name Code or subject number Address Any national numbers Any third party numbers Subject initials
Epidemiology Database	Subject name Code or subject number Partial address i.e. some geographic data retained such as area designation but not street or house number Any national numbers Any third party numbers Subject initials * But hospital admission and discharge dates can be retained

Other factors that may need to be addressed in certain circumstances to achieve an acceptable level of anonymisation are as follows:

- **Direct identifiers**

  Patient's name, address, health service number, contact details, photographs of people's faces (or other body parts where these could identify an individual e.g. a unique scarring) and unique administrative codes should be avoided

- **Patient geography**

  Geographic location should be no more specific than at the locality level

- **Physician identifiers and geography**

  Physician's identity and location should be concealed to avoid leading to the identity of the patient. In certain cases this may include indirect identifiers such as age of doctor, year of qualification etc

- **Extreme values of patient characteristics**

  Extreme values for age, height and weight should be avoided or masked

- **Rare conditions**

  A rare disease is one having a prevalence of less than 1 per 2000 population. Some kind of masking or aggregating of the information is recommended but different solutions may be needed in different cases

- **Event date information**

  Date of birth should be limited to month and year where possible. An alternative is to assign the first of the month to the date. However this may not be possible for birth dates for neonates and young children

  Recording of day, month and year for other events is acceptable unless they relate to the birth date

- **Specific socio-economic information**

  These include specific occupation, number of children, marital status, sexuality, nationality and family relationships. Generally these should not be collected but may be necessary in some cases

- **Free text**

  Free text may lead to the identification of the patient. Care should be taken with the text or it should be coded or filtered free of critical words at source

PART 3: GENERAL

SECTION VII: Security of Data

Security of data collected should be maximised to ensure that the requirements of the Data Protection Act 1998 are maintained:

- Access should be restricted to those employees of the sponsor (or organisations acting on behalf of the sponsor) who are directly involved in the **secondary** processing of data. Access to the data by other departments within the sponsor organisation (or organisations acting on behalf of the sponsor) should not be permitted and SOPs should be put in place describing how such access should be controlled
- Data should be retained for a time period sufficient to ensure regulatory or internal requirements are met and should be destroyed after this time period. Retention times for research material are likely to be relatively long and may therefore accommodate research on historical material
- Data should be encrypted when being transferred electronically within the sponsor organisation or to companies acting on behalf of the sponsor
- Firewalls and other internet security provisions should be in place before data are processed and/or shared

The use of privacy enhancing technologies ("PETs") should be considered. These include programs which encrypt or scramble data, and can allow researchers more extensive use of medical records with less risk that an individual's details will be disclosed through misuse or accident. They can operate at different levels and could permit support staff to have the necessary access to perform administrative tasks, without details of patients' medical conditions being disclosed. The Information Commissioner has issued a Data Protection Technical Guidance Note on Privacy Enhancing Technologies.

SECTION VIII: Data Protection Specialist or Officer

There is no legal requirement in the United Kingdom for a data controller to appoint a data protection officer. However as the legal framework regarding the use of personal data is complicated, it may be prudent to appoint a dedicated specialist for this purpose.

For example, where the handling of personal data extends beyond the bounds of the United Kingdom a set of inconsistent national and international laws and regulations adds further complication. Secondary research of personal data collected in more than one country will require compliance with the laws and regulations of each country where the data is collected or used. Even within Europe, there are inconsistencies in the way in which the Directive has been implemented. For example, in a number of countries, key-coded data is deemed to be personal data and therefore subject to local data protection laws, even where the data controller has no access or likely access to the key-code. In other countries (such as the UK) key-coded data is not personal data if the data controller does not have access or likely access to the key-code. It is therefore recommended that each data controller should ensure that he has the necessary understanding to meet full compliance with the law.

SECTION IX: Data Controllers Outside the UK

Where clinical trials are carried out by CROs in the UK acting for companies based outside the EU, it will be necessary to decide whether the company commissioning the research is a data controller 'established' in the UK for the purposes of Section 5 of the 1998 Act. If so, that company will need to ensure that it is notified as a 'data controller' under the Act. The role of the CRO will be that of 'data processor'. In some circumstances the CRO itself may, however, be the data controller.

SECTION X: Definitions

"Coded" means data associated with a subject but which is linked to an individual by a code.

"Anonymised" means that the link between the individual and the personal data has been destroyed and there is no way of identifying the individual. This can be achieved by a process of removing any direct identifiers and severing any link between the individual and the data.

"Medical Data" means a collection of information relating to the diagnosis, care and treatment of patients. Medical data can be personal data if it relates to an identified or identifiable individual.

"Secondary Processing" of data is defined as the processing of data for any research purpose other than that communicated to the data subject when the data was initially collected.

APPENDIX 1:
THE LEGAL FRAMEWORK

1. An overview of the Legislation

Medical research is governed by an overlapping set of legislation and regulations which, directly or indirectly, set down rules regarding the collection, storage and use of medical data. The Common Law Tort of Breach of Confidence also has an impact in this area.

The principal piece of legislation is the Data Protection Act 1998 (the "Act"), which gives effect in the United Kingdom to EC Data Protection Directive 95/46/EC (the "Directive") and replaces the Data Protection Act 1984. Important subordinate legislation has also been implemented which may have a direct impact in the area of medical research.

The Act applies only where a "data controller" is "processing" "personal data". Each of these terms is defined and is crucial to an understanding of the scope of the Act:

a "**data controller**" is a person who determines the purposes for which and the manner in which any personal data are, or will be, processed

"**personal data**" are 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. Personal data includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. The Act applies where personal data are processed using electronic means (e.g. on computer) and where personal data are held in manual form (e.g. in a structured filing system). The filing system must be made up of a set of information which relates to individuals either by reference to them (e.g. by name) or by reference to criteria relating to them (e.g. employee number), in such a way that specific information within that file about that individual is readily accessible

"**processing**" means virtually any activity performed in relation to data, such as obtaining, recording, holding, adaptation, alteration, retrieval, consultation, use, disclosure, blocking, erasure or destruction

"**sensitive personal data**" includes data which relate to the physical or mental health or condition of data subjects or their racial or ethnic origin.

Where a data controller processes personal data, he must comply with Eight Data Protection Principles that set out necessary standards for the processing of personal data. These principles are described in more detail in the next section.

The Act only applies to the processing (i.e. collection, use, disclosure etc) of *personal data* and *sensitive personal data*. This means that medical research which involves the processing of anonymised or coded data (see details in next paragraph) does not have to comply with the Act because such processing does not involve any data in the possession of the data controller that can identify a living individual. This is a crucial point for secondary research which is why the issue of anonymisation and what is meant by that term is discussed in more detail in section VII.

Personal data which are anonymised or coded are data which cannot identify an individual, either from the data themselves or from that data and other information which is in the data controller's possession or likely to come into his possession. ***A key issue is not whether the data controller will link the two sets of data together, but whether or not he can. Key-coded data will not be classified as personal data in the UK when it is in the hands of a data controller who does not have or is unlikely to have access to the key-code because it is unlikely that a clinical trial sponsor will have physical access to any information which serves to identify a patient.***

Data controllers who are multi-national organisations or have ties with other EU companies should take local legal advice on the application and interpretation of the base Directive in the Members States in which they operate to ensure compliance with specific legislation.

2. The Data Protection Principles

Data controllers may only process personal data if they do so in compliance with the Eight Data Protection Principles set out in the Act Section 4 (4) . These principles require controllers to:

1. process personal data fairly and lawfully and only if such processing can be justified under one of a number of prescribed conditions
2. process personal data only for specified, lawful and limited purposes
3. ensure that personal data are adequate, relevant, and not excessive in relation to those purpose
4. ensure that personal data are kept accurate and where necessary, up to date;
5. ensure that personal data are not kept longer than necessary
6. process personal data in accordance with data subjects' rights
7. put in place adequate security measures to safeguard personal data against unauthorised or unlawful processing
8. only transfer personal data to countries outside the EEA that provide an adequate level of data protection

The following sections consider in more detail some of the key principles and how they apply to the processing of personal data for secondary purposes.

3. The First Data Protection Principle

The First Data Protection Principle states:

> *"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."*

The term "*sensitive personal data*" is defined by the Act and includes data that relate to the physical or mental health or condition of data subjects.

The First Principle effectively imposes a prohibition on the processing of **any** personal data unless such processing can be justified. Where such processing is justified, the data controller must carry it out both fairly and lawfully.

A data controller processing data for medical research purposes will usually be processing sensitive personal data (unless those data are anonymised) and will therefore need to justify his processing under both Schedules 2 and 3. Given that Schedule 3 imposes additional conditions to those under Schedule 2, it is generally going to be the case that if the data controller can satisfy one of the conditions in Schedule 3, he will also be able to satisfy one in Schedule 2.

The Schedule 2 conditions which are most likely to be of relevance are:

- The data subject has given his consent to such processing
- The processing is necessary for compliance with any legal obligation (other than one imposed by contract)
- The processing is necessary in order to protect the vital interests of the data subject
- 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 because it causes prejudice to the rights and freedoms or legitimate interests of the data subject

The Schedule 3 conditions which are most likely to be of relevance in this area are set out below. A data controller may process sensitive personal data where:

- the data subject has given his explicit consent to such processing
- the processing is necessary to protect the vital interests of the data subject or another person, where it is not possible to get consent
- the processing is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), obtaining legal advice, or otherwise necessary for the purposes of establishing, exercising or defending legal rights
- the processing is necessary for medical purposes where these are undertaken by a health professional or a person owing a duty of confidentiality equivalent to that owed by a health professional. "Medical purposes" includes preventative medicine, medical diagnosis, medical research, provision of care and treatment and the management of healthcare services
- the processing of medical data or data relating to ethnic origin for monitoring purposes
- processing which is in the substantial

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

4. The Necessity Test

Many of the conditions for processing specify that the processing must be "necessary" for the particular purpose. The Information Commissioner has provided guidance that "in order to satisfy one of the conditions other than processing with consent, data controllers must be able to show that it would not be possible to achieve their purpose with a reasonable degree of ease without the processing of *personal* data. Where data controllers are able to achieve, with a reasonable degree of ease, a purpose using data from which the personal identifiers have been removed, this is the course of action that they must pursue"[1] . What constitutes a "reasonable degree of ease" is to be determined by taking into consideration issues including the technology available and the form in which the personal data are held.

5. The Requirement to Collect Personal Data Fairly

One of the requirements of the First Principle is that personal data must be processed fairly. In order to do that, the data controller must provide to the data subject certain information describing the processing of his personal data[2]. This information is usually provided by way of a data protection notice which can be inserted into consent forms. Integration of data protection obligations with consent forms is an approach favoured by the Information Commissioner's Office. The information to be provided (referred to as the "fair processing information") is as follows:

- the identity of the data controller
- the purposes for which the data are to be processed, including a description of any non-obvious or secondary purposes
- any other information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable the processing of the respective data subject to be fair. For example, data controllers may wish to inform data subjects of their right to subject access under the Act and their right to correct inaccuracies in their data. Data controllers may also, in order to ensure their processing is fair, be required to provide information regarding the types of recipients of the data and the purposes for which they would process the personal data

In the context of medical research, it should be relatively easy to comply with the obligation to provide the fair processing information in the context of the initial collection and use of personal data. It may be rather more problematic in respect of the use of personal data for a secondary purpose which may not have been considered at the time of the initial collection and which will not, therefore, be described in the original fair processing information.

The Act recognises that the provision of fair processing information presents some difficulties when data is obtained other than from the data subject and therefore provides for some exemptions from the obligation to provide the fair processing information where personal data about a data subject are obtained from a third party. In this limited situation a data controller is not obliged to provide the fair processing information where:

- doing so would require a disproportionate effort
- it is necessary for the data controller to process the data subject's personal information in order to comply with a legal obligation(other than where such obligation is merely imposed by contract)

The term "disproportionate effort" is not defined by the Act. In assessing what does or does not amount to disproportionate effort, the Information Commissioner has commented[3] that the starting point must be that data controllers are **not** generally exempt from providing the fair processing information simply because they have not obtained data directly from the data subject. What does or does not amount to disproportionate effort is a question of fact to be determined in each and every case.

The Commissioner will take into account a number of factors, including the nature of the data, the length of time and the cost involved to the data controller in providing the information. The fact that the data controller would have to expend a substantial amount of effort and/or cost in providing the information does not necessarily mean the Commissioner will reach the decision that the data controller can legitimately rely upon the disproportionate effort exemption. The above

1. "Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998", May 2002, page 8
2. Paragraph 2, Part II, Schedule I, Data Protection Act 1998
3. "Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998", May 2002, page 8

factors will be balanced against the effect on the data subject and in this respect a relevant consideration will be the extent to which the data subject already knows about the processing of his or her personal data by the data controller.

Where a data controller intends to rely on the disproportionate effort exemption, it should internally document that it is doing so and the reasons why it feels the exemption applies.

6. The Second Data Protection Principle

The Second Data Protection Principle states:

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

The Second Principle would seem to prohibit secondary use of personal data. The Act however provides a number of exemptions from the Second Principle, most notably where personal data are processed for the purposes of research (including statistical or historical purposes. This exemption, known as the "Research Exemption"[4] applies where the following conditions are met:

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

Where the Exemption applies:

- the further processing of personal data will not be considered incompatible with the purposes for which they were obtained
- personal data may be kept indefinitely **and**
- subject access does not have to be given provided that the results of the research or any resulting statistics are not made available in a form identifying the data subject

It is important to note that even where the exemption applies, the data controller is still required to comply with the rest of the Act, including the First and Second Principles. The data controller must ensure that, at the time personal data are collected, the data subject is made fully aware of the purposes for which the data controller intends to use the data. If the data controller subsequently decides to process the data in order to carry out further research of the kind that would not have been envisaged by the data subject at the time the data was collected, then the data controller must either seek the data subject's consent to such change of purpose, or rely upon the Research Exemption (if it can satisfy the conditions).

The following examples illustrate the application of the Research Exemption:

- records based research (for health economics or outcomes research) is proposed to be carried out using current patient records or ones yet to be created. In this situation, patients should be informed, as part of the standard fair processing information prior to initial collection, that their data may be used for research purposes designed to better understand and treat their conditions. Patient consent will be obtained for these purposes. As these records will have been compiled both for the purposes of treatment and research, the Research Exemption is not required
- records based research is proposed using existing records of patients who are no longer being treated for their condition. Such records may be quite old. The Research Exemption is required to enable this data to be used for research purposes, providing that the conditions described above apply

It is important to remember that neither compliance with the Second Principle nor the application of the Research Exemption remove the obligation to comply with the first principle. In both scenarios, researchers will need to give patients the fair processing information describing how their personal data are to be used unless doing so would involve a disproportionate effort (see page 16 "5. **The Requirement to Collect Personal Data Fairly**" for more information on the meaning of "disproportionate effort").

7. The Third, Fourth and Fifth Data Protection Principles

The Third, Fourth and Fifth Data Protection Principles are discussed together as they all broadly relate to data quality and retention. Personal data:

3. must be adequate, relevant and not excessive in relation to the purpose for which the data are processed (*Third Principle*)
4. must be accurate and, where necessary, kept up to date (*Fourth Principle*)

4. The Research Exemption is set out in Section 33 Data Protection Act 1998

5. must not to be kept for longer than is necessary for the purpose for which those data are processed (*Fifth Principle*)

Where the Research Exemption applies (see previous section), it also provides an exemption from the Fifth Principle. Personal data which are processed for research purposes (in compliance with the relevant conditions) may, notwithstanding the Fifth Principle, be kept indefinitely.

8. The Sixth Data Protection Principle

The Sixth Principle imposes a statutory duty upon data controllers to process personal data in accordance with the rights of data subjects under the Act. These rights relate to:

- the right to access a data subject's personal data (*Section 7*)
- the right to prevent processing likely to cause damage or distress (*Section 10*)
- the right to prevent processing for the purposes of direct marketing (*Section 11*)
- rights in relation to automated decision-taking (*Section 12*)

9. The Seventh Data Protection Principle

The Seventh Data Protection Principle states:

> *"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."*

This principle requires data controllers to put in place adequate security measures to protect personal data. These security measures fall into two categories:

- **technical measures** - these may include software controls to restrict access to computer systems, passwords, methods of authenticating users, virus checking software, firewalls, encryption software and audit trails
- **organisational measures** - these may include restricting access to buildings, computer rooms, desks and equipment, training staff on the care and handling of personal data, checking staff credentials, putting in place a disaster recovery plan and ensuring appropriate security policies are in place

The level of sophistication of the technical and organisational measures must be commensurate to the level of harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage of the personal data. The type of personal data must also be taken into account - the more confidential or sensitive the personal data, the higher the level of protection that should be put in place.

Data controllers are also obliged to take precautions with regard to any third parties which they use to process personal data on their behalf ("data processors"). These data processors may be appointed to carry out research or to assist with the conduct of a clinical trial or simply to supplement the data controller's workforce. The Act requires data controllers wishing to use data processors to:

- choose data processors who can provide sufficient guarantees about the technical and organisational security measures they will use when they process the personal data
- ensure they have a way of checking whether the data processor is complying with the technical and organisational measures (e.g. by giving the data controller a right of audit)
- put in place a contract in writing with the data processor in which the processor agrees to act only in accordance with the controller's instructions and to comply with equivalent obligations to those set out under the Seventh Principle

Where a data controller appoints a data processor who is based outside the European Economic Area, the controller may wish to put in place one of the model contracts approved by the European Commission to enable transfers to take place to non-EEA countries. This is covered in the following section.

10. The Eighth Data Protection Principle

The Eighth Data Protection Principle provides:

> *"Personal data shall not be transferred to a country or territory outside the European Economic Area[5] unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."*

The European Commission has designated certain countries outside the EEA as providing an "adequate level of protection" (at the time of writing, these include Argentina, Canada, Guernsey, Isle of Man and Switzerland). Transfers to all other countries outside the EEA, including the United States, must comply with the eighth principle unless one of the exemptions applies (see below). If the further research is to be carried out outside the EU and the patient's consent

5. The EEA comprises the 25 Member States, plus Norway, Iceland and Lichtenstein.

was obtained prior to the introduction of the Act in 1998, check the scope of that original consent as it is unlikely to permit transfer of personal data outside the EEA.

The Act sets out a number of exemptions from the application of the Eighth Principle. The most relevant of these for the purpose of processing personal data for secondary purposes are:

- the data subject has given his consent to the transfer
- the transfer is necessary for the purpose of, or in connection with, any actual or prospective legal proceedings, obtaining legal advice or establishing, exercising or defending legal rights
- the transfer is necessary in order to protect the vital interests of the data subject

If one of these exemptions applies, then the transfer may take place without regard to the Eighth Principle.

The issue of transfers to non-EEA countries is complex and whether or not a transfer can take place will depend on the particular circumstances of that transfer. According to the Information Commissioner's Guidance (The Eighth Data Protection Principle and International Data Transfers - 30 June 2006), a data controller who wishes to transfer personal data to a non-EEA country should ask himself a number of questions:

- has the country of destination been designated as providing an adequate level of protection by the European Commission?
- can an adequate level of protection be assured by some other means, such as by using the European Commission's model contracts, or (where the destination country is the US) by signing up to the Safe Harbor rules, or, for intra-company transfers, by signing up to corporate binding rules?
- does the country of destination provide adequacy for the transfer in any other way? This involves having regard to a number of factors set out in the Act[6] which may help to identify whether an adequate level of protection can be provided. These factors include a consideration of the laws of the destination country, the nature of the personal data being transferred, any relevant codes of conduct and any security measures taken
- do any of the exemptions apply? If they do, then the Eighth Principle does not apply

If a data controller has worked through the above list of questions and not been able to answer "yes" to any of them, then the transfer may not take place. This is a key issue for any data controller who has a multinational structure and has in place global databases which share personal data (including clinical data) within group companies across various countries. Companies in this position may want to explore whether the companies in their group are able to devise Binding Corporate Rules to govern the transfer of personal data between the members of the group concerned.

11. Enforcement of the Data Protection Act

One of the Information Commissioner's obligations is to ensure compliance with the Act. The Commissioner has certain statutory powers to aid it in meeting that obligation. The three types of formal action open to the Commissioner are:

- service of an information notice or an enforcement notice
- bringing of a criminal prosecution
- obtaining and executing a warrant of entry

The Commissioner is required to provide reasons for the service of an enforcement notice and the data controller has a right of appeal. The Commissioner has also indicated that except in urgent cases, a preliminary warning will usually be given prior to the issuance of an enforcement notice[7].

A person who fails to comply with an enforcement notice is guilty of an offence and may be subject to payment of a fine on conviction. Where an offence under the Act is being committed by a company or other body corporate, a director, manager, secretary or similar officer of the body corporate may also be found guilty of the offence if it was committed with their consent or connivance, or attributed to their neglect. Prosecutions will be published in the Annual Report of the Information Commissioner which may result in negative PR for those organisations that are named.

The Information Commissioner has, [in the Regulatory Action Division notice of 2005] indicated that the nature of any enforcement action taken must be proportionate to the risk involved, particularly the risk of a breach of any fundamental rights of individuals. In considering enforcement the circumstances of each case will be taken into account. These could include:

- the seriousness of the breach
- damage and distress to the data subject
- the number of data subjects affected
- the circumstances of the data controller including the cost of compliance and the resources of the controller

6. These factors that identify whether the destination country provides an adequate levels of protection are set out in Paragraph 13, Part II, Schedule I, Data Protection Act 1998

7. Enforcement Statement, June 1999

12. The Common Law

The Common Law Tort of Breach of Confidence deals with unauthorised use or disclosure of certain types of confidential information and may protect such information on the basis of actual or deemed agreement to keep such information secret. There is a legal duty to not disclose confidential information, and a breach of that duty will give rise to a legal cause of action, where it can be shown that:

- The information in question has the necessary 'quality of confidence'. This means that the information should not be in the public domain or readily available from another source and that it should have a degree of sensitivity and value
- The information in question was communicated in circumstances giving rise to an obligation of confidence. The obligation of confidence may be express or implied from the circumstances such as where there is a special relationship between professionals, for example, relationships between doctors and their patients **and**
- There was an unauthorised use of that material. It seems that it is not always necessary to prove damage or detriment nor is it necessary to prove dishonesty

Confidentiality is not however an absolute right. The courts have generally recognised three circumstances in which the duty of confidence owed with regard to a particular information item may be ignored:

- where there is legal requirement (either under statute or a court order) to disclose the information
- where there is an overriding public interest (for instance, the information concerns the commission of a criminal offence or relates to life-threatening circumstances)
  or
- where the individual to whom the information relates has consented to the disclosure

There is little case-law in the field of secondary use of medical data since the majority of cases have arisen in relation to trade secrets. The Court of Appeal judgment in the *Source Informatics* case[8] does however provide some guidance. Source Informatics Limited wanted to collect information on what medicines were being prescribed by GPs and sell it to pharmaceutical companies. They proposed that this information be collected from pharmacists, but that patient names would not be disclosed. The Department of Health believed that even if patients' names were not disclosed, there would still be a breach of the duty of patient confidentiality held by pharmacists to patients since such information was not in the public domain and refused access to the information. The case went to the Court of Appeal which held that personal information *could* be used for public health research purposes provided that patients' names were not disclosed. The Court decided that patient confidentiality would not be breached if names were protected from disclosure. An argument based on breach of confidence was not a bar to Source Informatics proceeding. The Court did not take a view whether Source Informatics' proposal was in the public interest.

The Common Law Tort of Breach of Confidence pre-dates but continues to sit beside the legal framework of the Act and has not been removed by the passing of the Act. **It is therefore important to consider not only the application of the Act but also whether or not a proposed use of medical data complies with any Common Law Duties of Confidence.** There are also certain circumstances where the Act does not apply, but the Common Law does. The most notable example relates to data that identifies a deceased person: this will not be governed by the Act as the Act only applies in respect of living persons, but the Common Law Duty of Confidence can survive the death of the individual.

13. Section 60 of the Health and Social Care Act 2001

Section 60 of the Health and Social Care Act 2001 does not remove or reduce the need to comply with the provisions of the Act. Instead, it allows for a temporary setting aside of the Common Law Obligations of Confidence relating to medical records. This provision creates a power for the Secretary of State to make orders enabling the use and disclosure of patient identifiable information without the consent of the patients, where he considers it necessary or expedient (a) in the interests of providing patient care or (b) in the public interest.

The Secretary of State has established the committee, Patient Information Advisory Group (PIAG), to review proposals for research to be undertaken using personal patient data without obtaining the patient's consent. It is intended largely as a transitional measure whilst consent or anonymisation procedures are developed, and this is reinforced by the need to review each use of the power annually.

NB Section 60 of the Health and Social Care Act does not apply in Scotland or Northern Ireland.

8. R v Department of Health, ex parte Source Informatics Ltd [2001] All ER 793.

14. The Caldicott Principles

A report in 1997 entitled "Report on the Review of Patient-Identifiable Information" by the Caldicott Committee led to the establishment of the Caldicott Principles which will apply to either secondary research using personal data which is being undertaken by parts of the National Health Service, or secondary research being undertaken by anyone else using existing data sets (and stored samples) that include personal data and are held by the National Health Service.

The Caldicott Principles apply in addition to the requirements of the Data Protection Act 1998 and require each NHS Trust to appoint a 'Caldicott Guardian'. Permission must be obtained from that Guardian for the work to be undertaken. The Guardian will want to be satisfied on six counts:

Principle 1 - every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate Guardian

Principle 2 - patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s)

Principle 3 - where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out

Principle 4 - only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes

Principle 5 - action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality

Principle 6 - every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements

APPENDIX II

ACKNOWLEDGEMENTS

ABPI is grateful to the following for their contribution to the drafting and development of the Guidelines:

AstraZeneca UK Ltd:
Lucy Inger, Senior Counsel
Ellis Parry, Global Privacy Officer

GlaxoSmithKline Plc:
Russell Brooks, R&D Legal Operations
Dr. Sandy Chalmers, Director, Data Privacy Policy

IMS Health Incorporated:
David Trower, Chief Privacy Officer

Novartis Pharmaceuticals UK Ltd:
Malcolm Hunt, Head of Medical Excellence

Roche Products Ltd:
Elizabeth Owen, Compliance and Training Manager
Mandy Robertson, Legal Executive

sanofi-aventis:
Jackie Powell, Head of Clinical Operations