INTERNATIONAL ASSOCIATION OF CANCER REGISTRIES

Guidelines on Confidentiality for Population-Based Cancer Registration

Asian Pacific J Cancer Prev, **6**, 87-103

Confidentiality for Cancer Registries – Revised International Guidelines

Confidentiality in the context of health and biostatistical research concerns avoiding the disclosure of sensitive and identifiable information about individual patients to a third party. Confidentiality procedures have been the subject of change during recent decades. Patient treatment has increased in complexity, frequently involving both primary health care workers and specialists, often in several hospitals, and more health professionals require access to data on an individual patient to deliver proper medical care. Patient data that were once used almost exclusively by the treating physician are now often shared with others, including non-medical persons, to a far greater extent than in the past, particularly for research purposes. This research is generally intended for the benefit of the whole community, by identifying causes of disease, evaluating the outcome of treatment, assessing equity in health care and in access to treatment services, etc.

The availability and widespread use of computer systems to store, analyse and transmit large volumes of data, sometimes over public data networks, have radically altered the climate in which patient confidentiality must be maintained. These changes in the use of confidential data have coincided with heated debate on the ethics and the requirement for informed consent to the storage and use of personal health data. The ethical issue of confidentiality is more complex where the data subject is not contacted, and may no longer be alive, even if the results of the research do not enable the individual to be identified. This situation arises when data that are collected for purposes such as routine surveillance of disease or death, often under the aegis of government, or for hospital administration, or for occupational health, are collated from available sources and the records for a given individual linked for analysis. The results of such research may provide powerful new insights into trends in the health of the population without any need for individuals to be identified. The possibilities for computerised linkage of data for individuals, even for very large volumes of data, have increased public fears of misuse and of error, and they have stimulated a continuing public debate on ethics and confidentiality in health research.

The principle of informed consent however, is not practicable in much of the population-based public health research in which cancer registries participate, where, in principle, the whole population is under study. Hence, for research leading to publications of a statistical nature there is a need to preserve the possibility of linking data about a single person, while at the same time preserving the confidentiality of that person in the publication and handling phase.

Cancer registries have always observed and been concerned about the preservation of the confidentiality of the data on cancer patients entrusted to them. The International Association of Cancer Registries (IACR) devised a formal code of conduct to be followed by its member registries in the early 1990s, and the principles have been highlighted in IARC/IACR publications (IARC Sci Publ 95, 1991). These guidelines were revised by an ENCR Working Group (Storm et al., 2002) in the light of the EU Directive on the protection of individuals with regard to processing of personal data (Directive 95/46/EC, 1995) for the European cancer registries. On a global scale, such guidelines need to be revised from time to time, to be in line with new legislation, changes in society and in particular changes in the way data are handled. Improved computerised systems provide easier access and ever expanding possibilities of exploiting and sharing data. The aim of the present guidelines or code of conduct, is to update the previous guidance in the light of such changes, in order to secure a high level of security and confidentiality of cancer registry data on the one hand, while on the other hand preserving the ability to use the data for public health purposes as well as clinical and epidemiological cancer research.

The present guidelines are the result of a working group formed by the IACR with representation from different regions and cultures in the world. This document is not a set of rules, but should be considered in the light of the legislation, or lack of it, in the area where the cancer registry is situated.

The members of the working group were: Dr Hans Storm, Danish Cancer Society, Denmark (Chairman), Dr David Brewster, Scottish Cancer Registry, Edinburgh, UK, Dr Michel Coleman, London School of Hygiene and Tropical Medicine, London, UK, Dr Dennis Deapen, Los Angeles Cancer Surveillance Program, Los Angeles, USA, Dr Akira Oshima, Osaka Cancer Registry, Osaka, Japan. With the contribution of Dr Tim Threlfall, Western Australian Cancer Registry, Perth, Australia

Contents

Summary of Conclusions and Recommendations

A. Principles of confidentiality and the role of the cancer registry

A.1 The purposes for which data collected by the cancer registry are to be used should be clearly defined (section 3.5).

A.2 The legal basis of cancer registration should be clear and should ensure that all reporting bodies have legal authority to report cancer, whether registration is compulsory or voluntary (sections 3.2 and 4.3).

A.3 The cancer registry must maintain the same standards of confidentiality as customarily apply to the doctor–patient relationship; this obligation extends indefinitely, even after the death of the patient (sections 4.1 and 4.6).

A.4 Identifiable data may be provided to a clinician for use in the treatment of cancer patients (section 6.3), but only the data necessary for the stated purpose should be released (section 6.2).

A.5 Identifiable data may be transferred to a collaborating or central registry for the purposes of complete and accurate cancer registration (section 3.5.2).

A.6 The scope of confidentiality extends not only to identifiable data about data subjects and data suppliers, but also to other directly or indirectly identifiable data stored in or provided to the registry (sections 2.8 and 4.7).

A.7 Data on deceased persons should be subject to the same procedures for confidentiality as data on living persons (section 4.6).

A.8 Guidelines for confidentiality apply to all data regardless of storage or transmission media (sections 4.8, 5.6 and 5.8).

B. Measures for data confidentiality, protection and security

B.1 The Director of the registry is responsible for data security (section 5.1).

B.2 The staff of the registry should sign, as part of their contract of employment, a declaration that they will not release confidential information to unauthorised persons. This declaration should be renewed annually and will remain in force after cessation of employment (section 5.2).

B.3 Suitable control of access to the registry, both physical and electronic, and a list of persons authorised to enter the registry, should be maintained by the Director (section 5.4).

B.4 The Director should maintain a list of staff members indicating the nature and extent of their access to registry data (section 5.1).

B.5 Notices reminding staff of the need to maintain confidentiality should be prominently displayed (section 5.3).

B.6 Cancer registries should consider providing proof of identity to staff engaged in active registration (section 5.5).

B.7 Identifiable data should not be transmitted by any means (post, telephone, electronic) without explicit authority from the Director or a staff member to whom such authority has been delegated (section 5.6). Transmission by telephone should in general be avoided (section 5.7).

B.8 Cancer registries should consider the use of registered post or courier services for confidential data, as well as separating names from other data for transmission (section 5.6.1).

B.9 Precautions should be taken for both physical and electronic security of confidential data sent on magnetic or electronic media (section 5.6.2). This could be by separating identifying information from tumour-related data, or via encryption of the identifying information (section 5.8.1).

B.10 Use of the computer for confidential data should be controlled by electronic and, if possible, physical measures to enhance the security of the data, including use of a separate room, use of passwords, different levels of access to data, automatic logging of all attempts to enter the system, and automatic closure of sessions after a period of inactivity (section 5.8.1).

B.11 Demonstrations of the computer system should be performed with separate and fictitious or anonymised data sets (section 5.8.2).

B.12 Special precautions should be taken for the physical security of electronic back-up media (section 5.8.3).

B.13 Expert advice on security against unauthorised remote electronic access should be sought if necessary (section 5.9).

B.14 Measures should be taken to ensure the physical security of confidential records held on paper, microfilm, microfiche, and other electronic media (section 5.10), and to protect such data from corruption (section 2.10).

B.15 A policy should be developed for the safe disposal of confidential waste (section 5.11).

B.16 Security procedures should be reviewed at suitable intervals, and consideration should be given to obtaining specialist advice (section 5.12).

C. Release of registry data

C.1 Release of cancer registry data for research and for health care planning is central to the utility of the registry. The registry should develop procedures for data release that ensure the maintenance of confidentiality (sections 3.5 and 6.4).

C.2 The Director of the registry, a scientific committee or an external authority should be responsible for deciding if a request for identifiable data meets the requirements of the law and the registry's guidelines on confidentiality (section 6.1). The scientific soundness of the project should also be evaluated.

C.3 In the absence of written consent from data subjects and data suppliers, a cancer registry should not release identifiable data on data subjects or data suppliers for purposes other than research and statistics (section 6.2). National legislation with respect to confidential data should be observed.

C.4 Physicians should be given access to data needed for the management of their patients, if identified as such and if in accordance with national law (section 6.3).

C.5 The data subjects should be given access to their own data on request, unless a national law exempts such a release. It is however recommended that data subjects be advised to make the request via their own physician (section 6.5).

C.6 Enquiries from the press should be referred to the Director of the registry or to a staff member nominated for this purpose (section 6.7).

C.7 Requests for identifiable data to be used for research should include a detailed justification with a written commitment to adhere to the registry's guidelines on confidentiality, signed by the requesting party (section 6.4).

C.8 Registries should make available a document describing their procedures and criteria for the release of data (especially identifiable data) to researchers who request access to the data (section 6.4).

C.9 Cross-border transfer of identifiable individual data should only be carried out for a research project if allowed by national law, and if the level of protection is satisfactory (section 6.6).

C.10 It is recommended that advance plans should be made for the possible cessation of registry activity, including a description of procedures, variables, coding manuals, programs, etc., in order to maintain the subsequent utility of the database while safeguarding the confidentiality of its data (section 6.8).

1. Purpose of Guidelines on Confidentiality in the Cancer Registry

1.1 Background

The background for the original IACR guidelines is presented in a paper by Coleman et al. (1992). In brief, the code of confidentiality in cancer registration defines what information should be regarded as confidential, and describes measures of security, periodic review and surveillance of security procedures, conditions for the release of confidential data and protection of the individual's rights, including both the patient, the doctor and the hospital.

This revision of the guidelines was prepared to reflect changes in information technology and cancer registration procedures. Developments in information technology have raised concerns about confidentiality. These concerns and recommendations related to the protection of electronic health information have been dealt with by various experts and professional bodies (Anon., 2000; Lowrance, 2002; Lowrance, 1997; Medical Research Council, 2000; National Academy Press, 1997; Working Group to the Royal College of Physicians' Committee on Ethical Issues in Medicine, 1994).

The main objectives of confidentiality guidelines were outlined by Muir (in Jensen et al., 1991): (a) to ensure the protection of the confidentiality of data about individuals whose cancer is reported to the registry, so the information cannot reach unauthorised third parties; (b) to ensure that the cancer registry data are of the best possible quality; and (c) to ensure that the best possible use is made of the registry data for the benefit of cancer patients, the population and for medical research. A code of confidentiality helps in defining the proper balance between the right to privacy for the individual and the right of fellow citizens to benefit from the knowledge on cancer causation, prevention, treatment and survival, as derived from cancer registration. Guidelines may make clear to the public how cancer registries handle the data entrusted to them in confidence, as well as guiding registries in the creation of appropriate safeguards for all aspects of their operation, from data collection to analysis, and the release of data for research purposes.

1.2 Aims of this document

The aims of this document are to provide updated guidance on:

(a) The need for a code of conduct in the maintenance of confidentiality in cancer registration, and the definition of what should be considered confidential.

(b) The purpose of confidentiality measures in cancer registration, and their legal basis.

(c) The principles of confidentiality, including the measures to maintain and review security procedures.

(d) The use and release of registry data in accordance with these principles.

1.3 Data protection

1.3.1 Privacy

The right to privacy with respect to the processing of personal data (such as those required for cancer registration) is one of the fundamental rights and freedoms of a person.

1.3.2 Informed consent

Many of the uses of registry data, both in health care planning and in research, involve the use and release of identifiable data on individuals registered with cancer. Ideally, the processing and use of data should be underpinned by informed consent. Unfortunately, however, the need for informed consent would make it virtually impossible to use data from a cancer registry, for various reasons:

(a) The practical workload of seeking consent from the data subject each time data were processed would be a disproportionate burden for population-based cancer registries.

(b) The repeated burden to the patients and/or their relatives of being asked to consent is of concern.

(c) Seeking general consent from data subjects for whatever scientific and statistical use might be made of cancer registration data poses a further load on medical personnel, and has been known to cause an unacceptably low coverage of registration.

(d) From a legal point of view, consent can only be given for a limited period of time, whereas cancer registration data may be used in research decades after their collection.

(e) Differential withholding of consent can lead to bias that invalidates the data for any scientific purpose.

1.3.3 Derogation to the requirement for informed consent

National legislation or regulations may provide exemptions to the requirement for informed consent in the public interest. This does not necessarily override the requirement for data processing to be fair and lawful.

1.3.4 Derogation to the obligation to inform subjects about data processing

In principle, data subjects should be informed about the disclosure of personal/identifiable data to a third party. National legislation may exempt cancer registries from this requirement when the processing is for statistical, historical or scientific research, and the subjects cannot be informed (deceased persons), or provision of information would involve disproportionate effort. Notwithstanding any such legislation, it is good practice for registries to make every reasonable effort to inform the public of their existence, their modus operandi and their scientific and public health functions. In conclusion, cancer registries may operate without informing data subjects individually about processing and disclosure.

1.3.5 Clinical use of data

Data release for clinical purposes may be included in the function of some cancer registries. These data will be used for the benefit of the individual cancer patient, and should be subject to national legislation concerning the transfer and release.

1.4 Use of guidelines

In order for cancer registry data to be of value for clinical, statistical and research purposes, the data recorded must be as complete, accurate and reliable as prevailing circumstances permit. Irrespective of any legislative measures, these standards of quality can only be achieved if both the public and the physicians and institutions treating cancer patients are confident that the data required are necessary for the objectives of cancer registration and medical research, and that confidential data will be adequately safeguarded.

These guidelines are not intended to be adopted en bloc as a fixed set of procedures for the maintenance of confidentiality in any particular cancer registry or without modifications required as a consequence of national legislation. Rather, they are intended to present the basic principles of confidentiality and to provide a set of measures from which a registry may select and reformulate, as appropriate, those measures considered to be most useful in the preparation or revision of a local code of practice on confidentiality.

The guidelines will need to be applied in different organisational contexts – some registries are independent institutions, others are part of an academic department in a university, or of a government health department. The parent body, if any, may impose rules or constraints on the operation of the registry, but the registry director should remain professionally accountable for ensuring the registry's adherence to these guidelines, as a minimum standard.
The applicability of these guidelines will be kept under review by the IACR, and amendments will be made as necessary.

2. Definitions

2.1 Cancer

The term 'cancer' is used in this document to cover all neoplasms and conditions suspected as such, as defined in the International Classification of Diseases for Oncology, third edition (Fritz et al., 2000).

2.2 Cancer registry

A cancer registry may be defined as an organisation for the collection, storage, analysis and interpretation of data about persons with cancer.

2.2.1 Hospital-based cancer registry

Cancer registries that limit their aims to recording the particulars of cancer cases seen in a given hospital or group of hospitals, irrespective of the geographical area of residence of the patients.

2.2.2 Population-based cancer registry

Cancer registries that aim to register details of every cancer that occurs in a defined population, usually in those persons resident within the boundaries of a defined geographical region or country.

2.2.3 General cancer registry

A cancer registry recording all types of cancer. Such a registry may be hospital-based or population-based.

2.2.4 Specialised cancer registry

A cancer registry recording only cancers of a given anatomic site, morphologic type or age group. Such a registry may be hospital-based or population-based.

2.3 Cancer registration

Cancer registration is the process of the continuous, systematic collection of a defined data set on the characteristics of all persons diagnosed with cancer, and of the characteristics of the cancer, including its treatment and outcome.

2.4 Data subject

An identified or identifiable natural person, on whom information is processed.

2.5 Privacy

Privacy may be defined as the right of a person to keep personal information about themselves secret. Respect for privacy means that a person should not normally be expected to reveal personal information, medical conditions, or behaviour unless s/he chooses to do so. Deliberate breach of an individual's privacy requires an ethical justification, for example, where it can be argued that such a violation may protect others from greater harm.

2.6 Informed consent

Informed consent may be taken to mean any freely given, specific and informed indication of the wishes of the data subject by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

2.7 Confidentiality

In this context, confidentiality may be defined as the set of constraints that apply to health information of a private or sensitive nature, which a person has chosen to reveal to a treating physician (section 2.13) or healthcare professional but which should not be revealed to others. Confidential information should not be shared with anyone without consent except when there is a clear ethical justification, or a legal requirement to do so. Research use of identifiable data without consent requires a demonstration of the importance of the research, minimal risk to the data subject, promise of benefit to society and a professional obligation to maintain the confidentiality of the information.

2.8 Confidential data (personal data)

For the purposes of this document, any data collected and stored by a cancer registry which could permit the identification of an individual patient (data subject) or, in relation to a particular data subject, of an individual physician or institution (data supplier) are considered to be confidential. An identifiable person is one who can be identified directly or indirectly by reference to a reference number or other identifying information such as names, date of birth, etc. held in the registry database.

The collection of identifiable information on the data subject is necessary to ensure the quality of the data held by the registry. The dates of birth, diagnosis and death are needed for many purposes related to public health surveillance or research. The data which, in association with a cancer diagnosis, are considered as confidential either alone, or in combination with other data items, are listed below:

(a) Names

(b) Unique reference numbers (e.g. national identity numbers)

(c) Address

(d) Full date of birth, if combined with sex and small area code for place of residence or death

(e) Date of death, if combined with sex and small area code or full date of birth

In rare instances, the combination of age, sex, year of diagnosis and small area code may be regarded as confidential if the population in the area is sufficiently small. Some cancer registries work on the principle that patients may be identifiable if the population denominator is less than, or in the range of 500-1000, and strictly control the release of such data.

2.9 Security

Security denotes the physical measures taken to prevent unauthorised access to the registry data, irrespective of the medium or method of storage or transmission.

2.10 Data protection

Data protection includes both the prevention of physical access to the data (security), and the electronic measures taken to protect the data from unauthorised access or corruption during many years of storage.

2.11 Processing of personal data

Data processing denotes any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking and erasure.

2.12 Filing system

Denotes any structured set of personal data, whether physical or electronic, and whether centralised, decentralised or dispersed on a functional or geographical basis, that are accessible according to specific criteria.

2.13 Treating physician

The treating physician may be defined as the patient's General Practitioner (GP), the doctor primarily responsible for the patient's cancer treatment, the pathologist, or a doctor to whom the patient has been referred for additional investigation or treatment, or their professional successors. The medical director of the institution where the treating physician is or was employed when treating the patient in question may also act on behalf of the physician.

2.14 Controller

The data controller denotes the natural or legal person (Registry Director), public authority, agency or any other body that alone determines the purposes and means of processing personal data. When the purposes and means of processing are determined by laws or regulations, the data controller or specific criteria for his or her designation may be specified by law.

2.15 Processor

The data processor is a natural or legal person, public authority, agency or any other body that processes the personal data on behalf of the data controller.

2.16 Third party

A third party is any natural or legal person, public authority, agency or any other body than the data subject, the controller, the processor and the person who, under the direct authority of the data controller or data processor, is authorised to process the data.

2.17 Recipient

A data recipient is a natural or a legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not.

3. Role of the Cancer Registry

3.1 Function of the cancer registry

The cancer registry plays a central role in all aspects of cancer control (Muir et al., 1985), not only for the population covered but also for other populations with which results can be compared. The systematic collection, recording and analysis of data relating to the lifetime of identified individuals with cancer enables analysis and interpretation of clinical and pathological characteristics of cancer, cancer incidence, mortality, prevalence, recurrence and survival for various population subgroups. It also opens the way for epidemiological research into the causes of cancer, exposure to carcinogens and effects of interventions in prevention and early diagnosis, provided that patients can be identified and linked individually to other files. In many countries, the cancer registry has proved to be an important tool for public health surveillance, including the planning and evaluation of health services.

3.2 Legal basis of registration

Cancer registration may be based on compulsory or voluntary notification of cancer patients to the registry. The basis for compulsory registration may be legislation passed by a parliament or elected legislative body (primary legislation), or an administrative order issued under the aegis of a statutory agency such as the Ministry of Health or a provincial health authority.

If cancer registration is not required by law or administrative order, the registry should at least ensure that all reporting bodies have legal authority to report cases of cancer.

Some cancer registries may obtain both voluntary and compulsory notifications, depending on the source of information. In some areas, for example, pathologists report voluntarily, whereas the patient's physician in hospital or general practice is legally required to do so; in others, pathologists are legally required to report cancers to the registry, whereas treating physicians report voluntarily. Vital statistics offices may be legally required to report the vital status, and if deceased, the cause of death of cancer patients. Fulfilling a legal requirement to report cases of cancer may simply mean the data supplier allowing cancer registry staff access in order to abstract specified information (active registration). Alternatively, it may require the data supplier to provide the registry with copies of various documents from the patient records, or special cancer notification forms, or electronic notifications, whether by a dedicated electronic form or by extracting information that has already been computerised by the data supplier (passive registration).

If cancer registration involves automated data linkages between one or more patient-related registries, vital statistics registries or population registers, the cancer registry must ensure that these procedures are permissible under relevant

legislation. It is recommended that the data items included in these linkages be specified in the documentation of registry procedures.

3.3 Sources of information

Registries should collect only the most important data, and ensure that it is complete and of high quality (Jensen et al., 1991). Registries should also ensure that tumour data can be linked to other databases where necessary, for the purposes of quality control, public health surveillance and research.

Notifications of cancer may be derived from many sources, such as the treating physician, surgeon, radiologist or radiotherapist; hospital admissions and records departments, the hospital discharge report, or laboratories of pathology, cytology, haematology or biochemistry; medical records of social security systems, private or government health insurance systems, hospital patient registries or central patient registries and coroners and vital statistics offices (death certificates). Notifications may be submitted on paper records or on magnetic, optical or other machine-readable media, or may be derived from computerised data linkage between e.g. hospital-based patient registries, pathology registries and cause of death registries (vital statistics). In some areas, registry employees may visit the source of information to obtain notifications (active registration), whereas in others the sources of information may submit these directly to the registry (passive registration). Many registries use both active and passive methods of registration.

An important part of the information about the data subject may come from population registers, which confirm the identity of the data subject, date of birth, address and maybe occupation, and whether the subject belongs to the population to be covered by the registry (residency). Follow-up information on deaths or emigrations may also come from this source.

3.4 Data items

Cancer registries should observe the principles related to data quality and collect data that are adequate, relevant and not excessive in relation to purpose, as well as being accurate, complete and up to date. The number of data items should thus be limited for two reasons – quality (the fewer data items, the greater the likelihood that these will be recorded correctly) and confidentiality (the more data items, the greater the chance of an unintended breach of confidentiality when releasing data).

The data items in the recommended minimum dataset for cancer registries are listed in Table 1. This set of data items is subject to periodic revision.

3.5 Use of cancer registry data

The purposes for which data collected by the cancer registry are used should be clearly defined. Cancer registries are important sources of data, both for clinical purposes and for public health surveillance or research intended to advance the understanding of the causes, occurrence and outcome of cancer.

Data may be either identifiable or aggregate (anonymous), depending on the nature of the analysis. Some examples of the use of cancer registry data in relation to confidentiality are outlined below. This list is not intended to be exhaustive, but to identify some important categories of the use of registry data.

3.5.1 Quality of diagnosis, treatment and health care

The clinical use of identifiable data relating to patients registered with cancer arises in the context of their diagnosis, treatment and follow-up by the treating physician(s). The availability of identifiable data to the treating physician is essential to avoid the duplication of diagnostic procedures, to permit the exchange of information between treating physicians, and to allow the physician to evaluate the outcome of treatment in individual patients or in groups of

Table 1. Items of information collected by registries (from Jensen et al., 1991)

Essential variables	
Personal identification	Names (in full) AND/OR unique personal identification number
Sex	Male or female
Date of birth	Day, month, year
Address	Usual residence (coded)
Incidence date	At least month and year
Most valid basis of diagnosis	
Topography (site) of primary	ICD-O
Morphology (histology)	ICD-O
Behaviour	ICD-O
Source of information	
Recommended variables	
Date of last contact	At least month and year
Status at last contact	At least dead or alive
Stage or extent of disease	
Initial treatment	

patients. Identifiable data required for such clinical purposes may therefore be provided to the treating physician on request, and in accordance with the procedures outlined in section 6, in order to assist the physician in the management of his or her patients with cancer. Identification of the data subject is indispensable for this purpose. The registry and the physician should maintain the confidentiality of the personal information on the data subject during the transmission of data (see below).

3.5.2 Transfer of identifiable data for registration purposes

In two circumstances, registries may need to transfer identifiable data to other cancer registries for the purposes of complete registration, quality control and the avoidance of duplication. The first case involves a tumour diagnosed in a person who proves to be resident in the territory of another, usually adjacent, registry. The second case involves regional registries that contribute data to a larger or national registry, or specialised registries that also contribute data to a general population-based registry. In each case, data may be transferred for the purposes of complete and accurate registration, provided that the recipient registry adheres to comparable standards of confidentiality.

3.5.3 Use of identifiable data for public health surveillance or research

(a) Studies of the causes of cancer

Case–control and cohort studies help in identifying the causes of cancer. Both types of study require information about individuals with cancer. In a cohort study, for example, linking the cohort members against the cancer registry files (or against a file of death certificates) enables cancers and deaths arising in the cohort to be detected. This has proved a highly efficient, economical and confidential method of detecting risk. Such linkages may be manual, computerised or both, and whereas linkage always requires knowledge of the identity of individuals with cancer, irrespective of whether the identifiable information appears in encrypted form or not (see 5.8.1), the resulting publications always present anonymous or aggregated data. It is, however, important for quality control in such studies that the researcher can check the quality of the linkages and resolve spurious linkages, and for these purposes identifiable data must be available.

Registries are frequently used as a source of cases (and sometimes also of controls) for case–control studies. The value of these studies for identifying risk factors is enhanced by the availability of a representative sample of tumours diagnosed in the population. Any contact with data subjects should be undertaken through the treating physician or hospital, and with the approval of the relevant ethical committee(s).

(b) Evaluation of screening

Cancer registries play a major role in the evaluation of screening programmes, by providing information to enable the assessment of whether, in comparison with an unscreened population, invasive cancer, e.g. of uterine cervix, develops less frequently and mortality decreases in a screened population or subgroup. In particular, the complete identification of interval cancers requires the comparison of lists of individuals who have attended the screening programme with cancer registry files. The cancer registry is thus essential for adequate evaluation of a population-based cancer screening programme. Cancer registry files may also be useful in the follow-up of individuals participating in a screening programme, in order to assess the validity of the screening test.

(c) Evaluation of survival from cancer

By linking the registry files with population and/or death registers to obtain the vital status of all cancer patients, it becomes possible to assess the survival of all persons with cancer in a defined population. Population survival rates will usually differ from those reported from selected series of patients (e.g. clinical trials). Such data may be used to evaluate the extent and speed with which new or improved cancer treatments are incorporated into routine clinical practice. It is also possible to assess population survival rates by the extent of spread at diagnosis, or by the type of treatment, or by other variables such as area of residence or socio-economic status.

3.5.4 Genetic counselling

Population-based registry data can be used for the genetic counselling of individuals concerned about hereditary cancer. This is facilitated by the availability of data on cancer type, sex, and the age of affected family member(s) at diagnosis and/or death. Such use may however violate the privacy of any relative who is registered with cancer. The use of cancer registries for genetic counselling should therefore be based on informed consent from the data subjects involved. An example of how one country (the United Kingdom) operates in this context is shown in Annex 1.

3.5.5 Use of aggregate data

(a) Public health surveillance or research

One of the most important contributions of the cancer registry is to provide current data on the incidence of various types of cancer, and on variations in incidence by age, sex, place of birth, occupation, ethnic group,
and other variables. These data can also be used to study differences in histological types and between urban and rural areas, and to examine trends in incidence over time. Only aggregate, anonymous data are used in such studies.

(b) Health care planning

Information provided by the cancer registry on the numbers of cancer patients can help health authorities in various ways, including long-term planning for the provision of medical facilities and the training of health care professionals; the establishment of priorities and programmes for cancer control; evaluation of the effects of intervention; and estimation of the numbers of cancer patients in the future (projections). For most of these purposes, the identity of individual cancer patients is neither needed nor provided; only aggregate data are used.

4. Principles of confidentiality

4.1 Underlying concept of medical confidentiality

The set of principles outlined below relates to the preservation of confidentiality in connection with or during the process of collection, storage, use and transmission of identifiable data by the cancer registry. A cancer registry must maintain the same standards of confidentiality in handling identifiable data as apply to the doctor–patient relationship; this obligation extends indefinitely, even after the death of the patient.

These guidelines are intended to help ensure the confidentiality of data about individuals whose cancer is reported to the registry, so that information on registered persons cannot reach unauthorised third parties.

4.2 Sharing of confidential clinical information

For serious diseases such as cancer, 'in modern medical practice, the doctor can seldom be the sole confidant, since effective care involves others, both medical and non-medical, technical and clerical, who provide services and manage the health care institutions' (Medical Research Council, 1985). Despite this essential dispersion of confidential information within the clinical team, the ultimate responsibility for the maintenance of confidentiality remains with the treating physician. The treating physician who provides information to a cancer registry about a patient with cancer therefore has the right to expect that the registry observes strict rules of confidentiality (see section 5.1).

4.3 Legal protection of data suppliers

Unless cancer is a disease that must be notified to a cancer registry by virtue of a law or administrative order, the data recorded by the cancer registry are supplied on a voluntary basis by the physician or institution. In some countries, therefore, it may be necessary for the registry to ensure that there is at least legal authority for physicians to report cancer, in order to protect data suppliers from legal action for breach of confidentiality in submitting identifiable data to the cancer registry.

4.4 Confidentiality and utility

Effective operation of the cancer registry depends on the continuous supply of identifiable information from several sources, notably clinicians, pathologists, hospital patient registration systems and vital statistics offices. These data suppliers can only be expected to continue to provide such information if the cancer registry can be trusted to maintain the confidentiality of those data and to make appropriate use of the data. Data suppliers will therefore need to be satisfied that the registry adheres to an adequate set of guidelines on confidentiality, and that data of high quality are being collected and used for the benefit of cancer patients, public health surveillance and cancer research. It is important to ensure that the confidentiality procedures followed by the registry are compatible with national and relevant international legislation, and national professional guidance.

4.5 Scope of confidentiality measures

Maintenance of the confidentiality of identifiable data held by the cancer registry should extend beyond information on cancer patients (data subjects) and data suppliers, to include identifiable data about data subjects derived from medical records, census data, interview records, death certificates and lists of members of industrial cohorts or other study populations that may be stored in or provided to the cancer registry as part of its routine operations, for public health surveillance or for research.

4.6 Confidentiality of data on deceased persons

Data on deceased persons held in the cancer registry should be subject to the same procedures regarding confidentiality as data on living persons, even though death certificates or related information may be available from other sources, or even in the public domain. A national regulatory body may however exempt the release of data about deceased data subjects from this confidentiality constraint.

4.7 Indirectly identifiable data

Individual records from which names and address have been removed, but from which it might still be possible to identify an individual indirectly by the use of the remaining data, e.g. an identity number, should also be subject to measures for the preservation of confidentiality in the cancer registry.

4.8 Methods of data storage and transmission

Guidelines for the maintenance of confidentiality are applicable not only to the storage of identifiable data on computers, but also to the storage of such data in the form of paper records, microfilm, scanned images and magnetic media, and their transport or transmission by registry personnel in any of these formats. The procedures involved may differ, but the underlying principle is the same.
The transmission of confidential data by means of the internet, file transfer protocols, e-mail or by equivalent methods must be carried out in accordance with the recommendations in sections 5.6 and 5.8 below.

4.9 Ethics

Ethics in medical research are enshrined in the Helsinki Declaration and in the Nuremberg Codes of Conduct. A basic principle for the recording of personal data about living subjects is that the subject's consent should normally be obtained unless national legislation decrees otherwise. Population-based cancer registration is not feasible under a requirement for informed consent, and legislation such as the European Directive provides an exemption from this requirement for cancer registration (95/46/EC Article 8).

5. Measures for Data Confidentiality

5.1 Responsibility

The Director of the cancer registry is usually in legal terms the 'controller' or the 'processor', and is responsible for maintaining the confidentiality of identifiable data. The Director must ensure that both registry staff and any third parties working with the registry are aware at all times of their individual responsibilities with respect to confidentiality, and that the security measures adopted by the registry are known and adhered to by all parties. It is recommended that an up-to-date list of staff members and 'third parties' be maintained, indicating the type of data to which each of them has access, and that an adequate system of computerised security measures be put into place (see section 5.8.1). Further conditions for the release of data should also be met by the Director (see Section 6). Specific criteria for appointment of the Director as the person who is responsible for data privacy and security may be set out in law. If not, the criteria should be detailed in the Director's job description, and failure to comply with them should be considered a breach of the oath of secrecy (see section 5.2).

5.2 Oath of secrecy

Duly trained and specialised staff should be appointed to run the cancer registry in accordance with its aims and rules of operation. As part of their contract of employment or conditions of service, each member of the registry staff should be required to sign a declaration to the effect that they will not disclose confidential information held by the cancer registry or brought to their attention in the line of work (e.g. active registration) to an unauthorised person at any time, or to any other person except as permitted within the context of the registry's guidelines on confidentiality. The terms of the contract of employment should make it clear that a breach of this undertaking will result in disciplinary action, which may involve dismissal. The declaration should be updated as necessary and should be signed annually by each employee. The declaration may specify sanctions such as disclosure of any previous breach of confidentiality by the employee, if a potential employer were to request evidence of good conduct. This declaration of secrecy shall remain in effect even after the staff member ceases to be employed in the cancer registry.
For staff involved in active cancer registration (see section 5.5), it is recommended that they are made aware of, and sign, the confidentiality rules of each data provider, and that these rules and declarations are attached to the general oath of secrecy kept in the registry.

5.3 Display of reminders

It is recommended that notices reminding staff of the need to maintain confidentiality be prominently displayed within the registry.

5.4 Physical access to the registry

Unauthorised access should be prevented. Physical access to the registry premises should be controlled by adequate technical safeguards. Suitable locks and alarm systems should be installed to control physical access to the registry. Consideration should be given to the use of special locks with entry codes, or electronic methods of controlling access, and to the maintenance of a record of persons other than staff members who enter the registry. The Director of the registry should maintain an up-to-date list of all persons authorised to enter the registry.

5.5 Active registration

Registry staff who are assigned to active registration duties, i.e. collecting information at health care facilities (sources), are responsible for maintaining the confidentiality not only of identifiable data they may collect on persons with cancer for the registry, but also of other information of a confidential nature that they may read or hear at the source (see section 5.2).

Cancer registries using active methods of registration should give consideration to the safe transport of confidential information (see section 5.6), to measures to avoid the accidental loss of such material, e.g. by keeping a back-up at the source, and to providing staff with suitable means of identification as an employee of the cancer registry.
The identity of such staff should be made known to the relevant person(s) at each of the sources that they visit to collect information for the registry. Changes in personnel should be notified to these sources in advance of any subsequent visit by the new staff member.

5.6 Transmission of information

Authority to transmit identifiable data from the registry, irrespective of the method, must be given by the Director (controller) or other nominated staff member to whom specific responsibility for such transmission has been delegated (processor).

5.6.1 Postal and courier services

If postal or courier services are needed for transfer of confidential information, be it on paper or electronic media, consideration should be given to the use of registered post or other forms of recorded acceptance and delivery by the service. The identifiable information should be transmitted separately from the health information, for subsequent linkage by authorised staff upon receipt of both transmissions, using internal codes.

For data on electronic media, the encryption of identifiable information with a special key is an alternative to the procedure of two separate transmissions (see also section 5.8.1).

The use of double envelopes, the external envelope giving a general address, and the internal envelope being marked for opening only by a named individual, is a precaution against accidental access to the information by unauthorised personnel.

If a courier service is officially authorised to handle confidential data and is used, the registry may consider if derogation from the procedure for separate mailing and encryption is acceptable.

5.6.2 Magnetic or electronic data transmission

When identifiable data are transmitted electronically or sent physically on magnetic or other machine-readable media, suitable precautions should be taken to ensure the physical security and the confidentiality of the material in transit. In addition to the steps taken to ensure that the data cannot easily be read by an unauthorised person, measures to check for incorrect or corrupt files must also be taken. Among the precautions that may be taken are:

(a) Encryption of names and other identifiable information at various levels of complexity, with a special key only available to authorised users (see also section 5.8.1).

(b) Sending the file, tape, diskette (etc.) containing names, address and other identifiable data separately from the media containing tumour-related or other data, using a link number to enable the reconstitution of the record by the intended recipient, and giving maximum security to the media containing identifiable data.

(c) Inclusion of tabulations and counts by which the content of the transferred data can be checked, as well as the program written to produce the tabulations and counts.

5.6.3 Processing and matching of data by external agencies

The registry files may need to be processed or matched against other computer files, either to provide missing data items or for the purposes of routine surveillance or research. If it is necessary for such processing to be undertaken outside the registry, e.g. in a vital statistics office or on an external computer, or in another country (see also section 6.6), the registry must ensure that the confidentiality of its records will be preserved by the agency receiving the registry data and that the measures used comply with the relevant national law. Data transmission should be in accordance with the procedures outlined elsewhere in this section.

Any unnecessary transfer of identifiable data outside the registry should be avoided.

5.7 Use of telephone

It must be clearly recognised that use of the telephone, although convenient, may easily give rise to a breach of confidentiality. It is under normal circumstances virtually impossible to document the content of a telephone conversation; hence it is difficult to handle in legal terms.

As a general rule, no identifiable data or confidential information of any kind should be given to telephone callers by registry staff.

The need for the registry to pass identifiable information to external callers by telephone should be infrequent. In rare instances in which the telephone method can be justified by the Director, the identity of the caller (name, position, title and address) must be checked and suitably documented, and a call-back procedure should be followed, using only officially published telephone numbers.

5.8 Use of computer

Physical and electronic measures should be used to prevent unauthorised access to information held on the computer. Electronic measures are subject to rapid evolution, and more effective solutions may emerge than those discussed in general terms here.

5.8.1 Access to data

(a) Workstations used for data access should be placed in a separate room(s), access to which is restricted.

(b) User names and passwords should not appear on the screen when typed.

(c) Passwords should be changed at intervals, and minimum requirements for changes (interval and password) should be specified in the registry code for confidentiality.

(d) An automatic log should be kept by the computer of all successful and unsuccessful attempts to enter the system, with regular checks of this log against written records of sessions spent at the terminal by authorised users.

(e) Different levels of access to the database, supported by password protection and user recognition, should be defined, such that only users authorised to gain access to identifiable data can do so. The Director should keep an updated list of persons who are allowed each level of access.

(f) Sessions which have been inactive for more than a short period such as 10 minutes should be automatically closed. Instructions should be given to staff to close sessions immediately after use.

(g) All testing of new hardware and software should be carried out with test data sets that have been either anonymised or are fictitious.

(h) Floppy disks and tapes that have held identifiable data must be efficiently erased or destroyed when taken out of use. Hard drives in computer hardware that is being decommissioned should be destroyed.

(i) Technical measures administered for the sake of data protection should not be allowed to compromise the quality of the basic data or make the use of the data unacceptably difficult or expensive.

5.8.2 Demonstrations

When the database and the computer system are demonstrated, fictitious or anonymised data should be utilised. Screen displays should be labelled appropriately to make visitors aware of this. A special data set for demonstrations is recommended.

5.8.3 Back-up

Back-up copies of the database should be made

frequently and regularly as a precaution to avoid loss of the database, and should be stored in a physically separate, safe location.

5.9 Unauthorised access to computer system

It must be recognised that some persons may attempt to gain remote electronic access to computer systems, often to show that this is possible rather than to examine the data. It is unlikely that registries using computer systems to which remote electronic access is possible can provide absolute protection against any such attempt at a reasonable cost. The level of security built in to such systems should at least be capable of foiling casual attempts to gain unauthorised access. Consideration should also be given to obtaining expert advice on enhancing the electronic security of such computer systems. This aspect of security should be regularly reviewed (see section 5.12). Although it may not always be possible, it is desirable that the cancer registry has an isolated data processing system.

5.10 Storage of original data

Electronic methods of storage of identifiable, validated and coded data in cancer registries are now almost universal, but most registries also store original data received on paper, either in paper form, copied on to microfilm, or scanned as images onto electronic media. Such material may include cancer registry notification forms, medical records, copies of pathology reports, copies of death certificates, etc. It is recommended that the original data be preserved for quality control, surveillance and research purposes, in line with the code of good conduct of the International Epidemiological Association for other research data. However, the storage of records on paper should be reduced to a minimum both for confidentiality and practical reasons. Paper records or copies thereof (irrespective of media) are accessible to casual or accidental inspection, and require no special expertise to gain access. Image-scanned files may be password protected, and are thus an exception.

Specific measures for paper records should therefore be considered, including:

(a) Defining who has access to the registry premises.

(b) Defining which members of staff have access to the room where confidential materials are kept.

(c) Providing lockable storage cabinets in which all confidential materials should be stored at the end of a working session.

(d) Ensuring that persons not authorised to do so (e.g. cleaning personnel) are not able to scrutinise paper or other physical records containing confidential data.

5.11 Disposal of physical records

A suitable policy should be developed for the safe disposal of waste paper and other physical records containing identifiable data, be it computer output or original data copied to either film or electronic media. The destruction of paper would normally involve shredding. This should preferably be performed within the premises of the registry. When the volume of confidential records to be destroyed is large, it may be necessary to employ specialised and officially authorised services for the safe disposal of confidential waste.

5.12 Review of confidentiality and security procedures

It is recommended that cancer registries undertake an annual review of their security procedures. This should include review of access files and logs. It should also include confidentiality training or updating sessions for all registry employees. At five-yearly intervals, it may be helpful to recruit the services of specialist advisers, in order to ensure that the registry's procedures for the maintenance of confidentiality are up to date. This should cover all aspects of the registry's operations.

6. Release of data

Only the data required for a specific purpose should be released.

Release of aggregate or anonymised data does not breach confidentiality. Care should be taken that a data subject may not be identified from anonymised individual records, e.g. by date of birth (age), sex, and residence in a small geographical area.

Many uses of registry data involve the release of identifiable data on individuals registered with cancer. National legislation or regulations may permit such release in the public interest.

National or international legislation may specify a requirement to inform the data subject about the disclosure of his or her data to a third party. Derogations from such a requirement may also be provided, for purposes such as public health surveillance or scientific research, or where the provision of such information is impossible (the data subject is deceased) or where it would involve a disproportionate effort.

Procedures must be developed to deal with requests for the release of confidential data. Examples of such procedures are given below.

6.1 Responsibility for data release

The Director (controller) should ensure that relevant legal and professional guidance is followed, and that confidentiality is preserved when identifiable data are released.

6.2 Limitations on data release

(a) National legislation with respect to data confidentiality should be observed.

(b) In the absence of written consent from all the parties concerned, a cancer registry should not release identifiable data either about a registered person (data subject) or, in relation to such a person, about a treating physician or institution (data supplier), for any purpose other than those outlined for clinical and research purposes (section 3.5).

(c) The data released should be limited to the variables needed for the stated purpose.

(d) Requests for information, even from physicians, may be received for identifiable data concerning individuals (who may or may not have a cancer recorded at the registry), from agencies such as pension schemes, health care cost reimbursement schemes or industrial disease compensation panels, or in the context of medical examination for life insurance or employment. Such requests should be refused, and the enquirer should be directed to obtain information directly from the subject or the subject's treating physician.

6.3 Release of identifiable data for clinical purposes

Access to identifiable data in the context of treating a registered cancer patient should normally be given to the treating physician, subject to national legislation concerning transfer and release of clinical data.

6.4 Release of identifiable data for scientific and health care planning purposes

The registry should prepare a public document setting out the criteria and procedures applicable to the release of identifiable data for research. This should include reference to relevant legal and ethical requirements. The document must be made available to researchers requesting identifiable data.

A request for the release of confidential data should be made in writing to the registry Director (example form attached, see Annex 2).The request should include:

(a) The purpose for which the data are requested.

(b) The information required, and a justification of any need for confidential data.

(c) The name and position of the person who will be responsible for the confidentiality of data obtained from the registry.

(d) The name and position of other persons who will have access to the registry's data.

(e) The period of time for which the data would be required, how the data would be used and how the data (and any copies) would be disposed of, returned or destroyed after the elapse of this period.

The requesting party should also provide a signed assurance to the registry director that the intended recipient of the identifiable data will:

(f) Observe the same principles and obey the same laws in relation to the identifiable data as observed by the staff of the cancer registry.

(g) Comply with all restrictions on the use of the data imposed by the registry, in particular that the data will not be used for purposes other than those agreed upon at the time of the provision of the data, and that they will not be communicated to other parties without explicit consent from the registry director.

(h) Not contact data subjects (or their relatives) whose identities have been provided in confidence by the cancer registry (e.g. for research based on interviews) unless a written authorisation to do so has first been obtained from the treating physician. When appropriate, approvals by ethical committees should also be sought.

(i) Ensure that no publication of the results will enable any individual to be identified.

(j) If the period of time exceeds 12 months, provide the registry director with an annual status report on the data.

(k) Report in writing to the cancer registry director when the data are disposed of, returned or destroyed as agreed.

(l) Give due acknowledgement to the registry for provision of the data in any publication or report.

(m) Provide the registry with a copy of all publications derived from use of the data.

6.5 Provision of data to individuals

Registries should not generally inform individuals whether or not data about them are held in the registry, but should divulge such information only through the treating physician. The reason for this is to avoid causing unwarranted anxiety to the patient and to ensure that they obtain medical advice and support when interpreting the information.

National law may exempt the data controller from releasing information to a data subject. Conversely, national law may require the cancer registry to inform a data subject, without excessive delay or expense, whether or not it holds data relating to him or her.

It is recommended that such data are released by registered mail to the data subject using double envelopes, a sealed one containing the print-out of the registry data and in the main envelope an accompanying letter advising the data subject to consult a physician when breaking the seal, in order to obtain proper guidance and advice in interpreting the cancer registry information.

6.6 Transfer of data across borders

When the study design requires that identifiable data be transmitted across registry or national borders, and if national legislation permits, such data can be transferred. The data should remain subject to the same rules of confidentiality as in the registry of origin. Cancer registries participating in such studies should satisfy themselves that their data will be treated accordingly, and should seek ap proval for the transfer from the appropriate authorities

Research projects involving the provision of data about individuals from many cancer registries, sometimes in different countries, have provided valuable information about cancer risk or outcome. Although it may be necessary for individuals to be identifiable within the context of such studies, identifiable data should not normally be transmitted to other registries or countries. Each subject may be allocated a suitable number by which his or her record can be traced in the cancer registry of origin by registry staff, for data verification and quality control. This number can then be used instead of the subject's identity in data files contributed to the study coordinating centre.

6.7 News media

Cancer registries are frequently approached by print or broadcast media for information on cancer. It is recommended that all such enquiries be referred to the Director, or to another nominated staff member who has been assigned specific responsibility for dealing with the press.

Great care should be taken not to disclose to the press personal data of any kind whatsoever, or any individual data that by linkage to other data (such as sex, age, small area) that could lead to disclosure of the identity of registered data subjects.

6.8 Cessation of cancer registration

Each cancer registry should develop a policy for the actions to be taken in the event that the registry ceases operation. Consideration should be given to methods of storage of the registry database in an archive, so as to preserve its utility for the purposes outlined above (section 3.5), while ensuring the maintenance of confidentiality. It is recommended that, where possible, a suitable agency such as a national or regional archive regulated by law be identified, in advance, to store the registry archive for a minimum of 50 years. This should include not only the registry data but also a description of the registry, including methods of data capture and handling, description of variables, quality control measures, code manuals, definitions and computer programs used, and a description of the structure of the archived file. The recipient archive should undertake to make the database available for the purposes defined by the registry and under the same rules of confidentiality as applied by the registry. Consideration should also be given to the data selected for storage and the method of archiving. Selected paper records might be microfilmed or image-scanned, and selected computer files archived on electronic media. The safe disposal of confidential records not included in an archive deposit should also be planned in advance.

References

Anderson RJ (1995). Security in clinical information systems. University of Cambridgehttp://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html) and BMA.

Anonymous (2002). United Kingdom of Great Britain and Northern Ireland. Privacy and human rights 2002: an international survey of privacy laws and developments, pp 375-92. London: EPIC and Privacy International.

Coleman MP, Evans BG, Barrett G. Confidentiality and the public interest in medical research - will we ever get it right? Clinical Medicine (in press).

Coleman MP, Muir CS, Ménégoz F (1992). Confidentiality in the cancer registry. *Br J Cancer*, **66**, 1138–49.

Cordier LJ (1995). The directive on the protection of individuals with regard to the processing of personal data, and medical and epidemiological research. *EU Biomed Health Res Newsletter May*, 5-7.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (1995). The protection of individuals with regard to processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, **281**, 31–50.

Fritz A, Percy C, Jack A, Shanmugaratnam K, Sobin L, Parkin DM, Whelan S (eds) (2000). International Classification of Diseases for Oncology, Third Edition, World Health Organization, Geneva.

IARC/IACR Guidelines on Confidentiality in the Cancer Registry (1992). IARC Internal Report No. 92/003. IARC, Lyon.

Jensen OM, Parkin DM, MacLennan R, Muir CS, Skeet RG (editors) (1991). Cancer registration – principles and methods. IARC Scientific Publication No. 95. IARC, Lyon.

Lowrance WW (1997). Privacy and health research. A report to the US Secretary of Health and Human Services. Washington, DC, DHHS.

Lowrance WW (2002). Learning from experience: privacy and the secondary use of data in health research. London, Nuffield Trust.

Medical Research Council (2000). Personal information in medical research. London, Medical Research Council. MRC Ethics Series.

Medical Research Council (1985). Responsibility in the use of personal medical information for research: principles and guide to practice. *BMJ*, **290**, 1120-4.

Muir CS, Démaret E, Boyle P (1985). The cancer registry in cancer control: an overview. In: The role of the registry in cancer control. Parkin DM, Wagner G, Muir CS (editors). IARC Scientific Publication No. 66. IARC, Lyon, pp. 13-26.

National Academy Press (1997). For the Record: Protecting Electronic Health Information. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. National Research Council, Washington, DC: National Academy Press. http://www.nap.edu/bookstore.

Royal College of Physicians Committee on Ethical Issues in Medicine (1999). Research based on archived information and sample JR Coll Physicians Lond, **33**, 264–6.

Storm HH, Clemmensen IH, Black RJ (1998). Survey of cancer registries in the European Union. IARC Technical Report No. 28. IARC, Lyon, 1998.

Storm H, Buiatti E, Hakulinen T, Ziegler H ENCR (2002). Guidelines on confidentiality in population-based cancer registration in the European Union. ENCR, Lyon.

Working Group to the Royal College of Physicians Committee on Ethical Issues in Medicine (1994). Independent ethical review of studies involving personal medical records. *JR Coll Physicians Lond*, **28**, 439-43.

ANNEX 1

Confidentiality of Cancer Registry Data
Genetic Counselling

The policy of the United Kingdom Association of Cancer Registries (UKACR) concerning the release of data for purposes of genetic counselling requires that a named registered medical practitioner shall be responsible for the confidentiality, use and security of data (see below).

Policy

(i) Requests for cancer registry information from registered medical practitioners working in genetic counselling clinics concerning living family members, related to a proband undergoing counselling should be accompanied by a signed consent form obtained from each family member (or their legal guardian) about whom information is requested. The consent form should permit the release to the named registered medical practitioner of information relating to cancer from medical and hospital records. The consultant and, where possible, the general practitioner responsible for the family member should be informed about the data release.

Information regarding living cancer patients should not be released without their signed consent.

(ii) Information regarding patients known to have died can be released to a registered medical practitioner for counselling purposes, upon request, without seeking consent.

(iii) Registered medical practitioners receiving cancer registry information must undertake to maintain the confidentiality of the data, keep it securely and release it only for counselling purposes. The duty of confidentiality relating to medical information extends beyond death and the above requirements must be adhered to for information relating to both living and deceased patients.

(iv) The information released for counselling purposes should consist of the minimum necessary to achieve the objectives required. In normal circumstances this would comprise: name, address, date of birth, date of diagnosis, cancer site, and histology, name and hospital of managing consultant and (for living patients) name and address of GP.

Name of Medical Practitioner responsible:

……
I declare that I understand and agree to act in accordance with the UKACR policy.

Signature……
Date……

Name and recipient if not the medical practitioner whose name is given above.

……

EXAMPLE ANNEX 2

APPLICATION/RELEASE FORM

1. Name of project
2. Organization responsible for the project
3. Person in charge (name, position, address)
4. Other persons with access to the data (details as in point 3)
5. Location of the project
6. Contact person (name, address, telephone, fax, e-mail)
7. Type of project
   duration (beginning, end)
   - definition of the data items requested from the cancer registry
   - other data to be used, and whether permission for their use has been received or applied for
8. Goal of the use of the data (attach project plan, appendix b)
9. Data security measures to be used
10. Fate of the cancer registry material received
    - to be destroyed: when, how
    - to be archived: when, how

I agree to handle the data according to the terms below:

1. The data may only be used for the purpose specified in the project plan.
2. The data may not be released to a third party.
3. The privacy of the individual persons included in the data file must be respected. Only authorized contacts with patients through a treating unit are allowed.
4. The data protection measures described must be adhered to.
5. The data must be destroyed or archived according to the project plan. A notification must be made when this takes place.
6. Any changes in the project plan, particularly with respect to the items reported on the application form, must be notified immediately, and a new application including the changes must be submitted.
7. A report focusing on confidentiality must be given within a year of finishing the project. No individual may be identified in this or in any other report based on the project.
8. Resulting publications should be presented to the cancer registry.
9. Acknowledgement of the data source should be included in the publications.

---------- ----------

Person in charge of the project Date, signature

---------- ----------

Other persons with access to the data to be released Date, signature

Appendix A. Project plan
Appendix B. Other permissions received
Appendix C. Ethical committee's statement
Appendix D. Short CV of the person in charge