Chapter II

Guidelines on confidentiality in population-based cancer registration in the European Union

Contents

- 3.5.4 Genetic counselling
- 3.5.5 Use of aggregate data
  - (a) Research
  - (b) Health care planning

4. Principles of confidentiality

- 4.1 Underlying concept of medical confidentiality
- 4.2 Sharing of confidential clinical information
- 4.3 Legal protection of data suppliers
- 4.4 Confidentiality and utility
- 4.5 Scope of confidentiality measures
- 4.6 Confidentiality of data on deceased persons
- 4.7 Indirectly identifiable data
- 4.8 Methods of data storage and transmission
- 4.9 Ethics

5. Measures for data confidentiality

- 5.1 Responsibility
- 5.2 Oath of secrecy
- 5.3 Display of reminders
- 5.4 Physical access to the registry
- 5.5 Active registration
- 5.6 Transmission of information
  - 5.6.1 Postal and courier services
  - 5.6.2 Magnetic or electronic data transmission
  - 5.6.3 Processing and matching of data by external agencies
- 5.7 Use of telephone
- 5.8 Use of computer
  - 5.8.1 Access to data
  - 5.8.2 Demonstrations
  - 5.8.3 Back-up
- 5.9 Unauthorized access to computer system
- 5.10 Storage of original data
- 5.11 Disposal of physical records
- 5.12 Review of confidentiality and security procedures

6. Release of data

- 6.1 Responsibility for data release
- 6.2 Limitations on data release
- 6.3 Release of identifiable data for clinical purposes
- 6.4 Release of identifiable data for scientific and health care planning purposes
- 6.5 Provision of data to individuals
- 6.6 Transfer of data across borders
- 6.7 News media
- 6.8 Cessation of cancer registration

References

Annex 1 Example of application/release form
Appendix A Terms for use of the data
Annex 2 Sample oath of secrecy

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 clarified and it should be ensured that all reporting bodies have legal authority to report cancer, whether registration is compulsory or voluntary (section 3.2).

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) observing that only the data necessary for the stated purpose are 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 2.5 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 unauthorized persons. This declaration should 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 authorized 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 (ID)

information and tumour-related data, or via encryption of the ID (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 anonymized 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 unauthorized 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 2.8).

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 authority should be made responsible for deciding if a request for identifiable data meets the requirements of the law and the registry's guidelines on confidentiality. Also the scientific soundness of the project should be judged (section 6.1).

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 Data on a subject must be provided to the subject upon request, unless a national law exempts such a release. It is 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 commitment to adhere to the registry's guidelines on confidentiality (section 6.4).

C.8 Registries should provide 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 If allowed by national law, cross-border transfer of identifiable individual data should only be carried out if required for the conduct of a research project 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 present guidelines for confidentiality in population-based European cancer registries build upon the guidelines published by the International Association of Cancer Registries in 1992. The background for these 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.

These guidelines represent a review consistent with the European Directive 'on protection of individuals with regard to the processing of personal data and on the free movement of such data' (Directive 95/46/EC), which provides the basis for national legislation for the protection of individuals with regard to the processing of personal data. The review was carried out with a view to the modernization of cancer registration procedures, from primarily a paper-based system to one based on computerized data capture and storage. New information technology promises to make accurate information more readily available at a lower cost, but also raises concerns from the point of view of confidentiality, because of the easy storage and dissemination of huge volumes of data. These concerns and recommendations related to the protection of electronic health information have been dealt with by various committees worldwide (National Academy Press, 1997).

The main objective of guidelines for confidentiality was 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 unauthorized 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 to 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 the document

The aims of this document are to give updated guidance in relation to the European data protection Directive, on:

(a) The definition of terms of relevance for cancer registration and the Directive text.

(b) The articles and exemptions in the Directive of relevance to cancer registration.

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

(d) The objectives of confidentiality measures in cancer registration, and their legal basis.

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

(f) Guidelines for the preservation of confidentiality; and for the use and release of registry data in accordance with these principles.

1.3 European Directive 95/46/EC on data protection

1.3.1 Privacy

The right to privacy with respect to the processing of personal data (e.g. cancer registration) is listed as one of the fundamental rights and freedoms of a person, and the protection of this right is the main objective of the European Directive 95/46/EC. Recommendations on ethical issues in research have been published; however these do not have the same status as a law (Directive).

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. The Directive 95/46/EC Article 7 indicates that 'informed consent' is needed unless this use is based on contractual, legal, vital and public interest. Furthermore, the Directive prohibits the processing of data 'concerning health' (Directive 95/46/EC, Article 8).

The informed consent principle makes it virtually impossible to use data from a cancer registry, for various reasons:

(a) The practical workload of seeking consent each time data are processed is a disproportionate and very heavy burden for population-based cancer registries.

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

(c) Seeking general consent for any scientific and statistical use of the cancer registration process poses a further load on medical personnel and may lead to unacceptably low coverage of registration (as seen in Hamburg).

(d) From a legal point of view, consent can only be given for a limited period of time.

(e) The proportion of non-coverage (resulting from differences in patterns of asking for or giving consent) may vary by population, and true differences in cancer incidence may become confounded by differences in the accuracy of registration.

1.3.3 Derogation to the requirement of informed consent

The derogations to the European Directive 95/46/EC (Articles 8.3 and 8.4 and further explained in recital 34 of the Directive; Cordier, 1995) legalize the processing of data by a health professional subject to professional secrecy, without informed consent, for preventative medicine, medical diagnosis, the provision of care or treatment or the management of health care services, including scientific research. This includes all elements enshrined in cancer registration. National legislation may add further exemptions in the public interest by law or legal order. This does not override the requirement for data processing to be 'fair and lawful' (see para. 3.2).

1.3.4 Derogation to the obligation to inform subjects about data processing

The Directive 95/46/EC Article 11.1 also specifies the need to inform the data subject about the disclosure of data to a third party at the time when data are disclosed. The registries, however, fall under the derogation in Article 11.2 when processing is for statistical, historical or scientific research, and the subjects cannot be informed (deceased persons), or provision of information involves a disproportionate effort, or disclosure of information is allowed by national law. In conclusion cancer registries can operate without informing data subjects about processing and disclosure. Member states shall in these cases provide appropriate safeguards that must be observed by registries.

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 the legislation concerning the transfer and release of clinical data in the country.

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 be achieved only 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 rconfidentiality in any particular cancer registry or without modification needed as a consequence of national legislation. Rather, they are intended to present the basic principles of confidentiality with a view to the European Directive 95/46/EC, 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 applicability of these guidelines will be kept under review by the ENCR, and amendments will be made as necessary.

2. Definitions

2.1 Cancer

The term 'cancer' is used in this document to imply 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 organization for the collection, storage, analysis and interpretation of data on persons with cancer.

2.2.1 Hospital-based

Cancer registries that limit their aims to recording the particulars of cancer cases seen in a given hospital or group of hospitals irrespective of boundaries of geographical areas are said to be hospital-based.

2.2.2 Population-based

Cancer registries that aim to register details of every cancer that occurs in a defined population, usually those persons resident within the boundaries of a defined territory or geographical region, are said to be population-based.

2.2.3 General cancer registry

Each of the two mentioned registry types (2.2.1 and 2.2.2) can be general if all cancers are recorded in the defined catchment area (hospital or population).

2.2.4 Specialized cancer registry

Each of the two mentioned registry types (2.2.1 and 2.2.2) can be specialized if registration is restricted to cancers of a given site group or age group in the defined catchment area (hospital or population).

2.2.5 Record linkage data register

A cancer registry which uses record linkage of already computerized and coded data; it may be any of the subtypes in 2.2.

2.3 Cancer registration

Cancer registration is the process of the continuing, systematic collection of data on the characteristics of all cancers and of the persons diagnosed with cancer, and is the basic activity of a cancer registry.

2.4 Data subject

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

2.5 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 (ID) information such as names, date of birth, etc., or to factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

The collection of unambiguous ID information on the data subject is necessary to secure quality and use of the registry. Furthermore, the dates of birth and death are needed for many research purposes, but may in many instances be sufficiently detailed by month and year. The data which, in association with a cancer diagnosis, are considered confidential alone, and in combination with other data items (x) are listed below:

(a) Names

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

(c) Address

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

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

(f) Small area code (x), combined with sex and 2.5.4 or 2.5.5.

In rare instances the combination of age, sex, year of diagnosis and small area code may be regarded confidential because a person might be identified if the

population in the area is sufficiently small. In the UK, cancer registries work on the principle that patients may be identified if the population denominator is less than 1000. Release of such data is strictly controlled.

2.6 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, or a doctor to whom the patient has been referred for additional investigation or treatment. 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.

2.7 Security

Security denotes the measures taken to prevent unauthorized access to the registry data, whether stored on paper, microfilm, microfiche or magnetic media, or transmitted by any of these means.

2.8 Data protection

Includes both the prevention of physical access to the data (security), and the protection of the data to avoid corruption during many years of storage. The term should in this context not be confused with confidentiality (privacy), the aim of which is to protect the individual from unauthorized disclosures.

2.9 Processing of personal data (Directive 95/46/EC definition)

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

2.10 Filing system

Denotes any means to achieve a structured set of personal data that are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

2.11 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 controller or the specific criteria for his or her nomination may be designated by law.

2.12 Processor

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

2.13 Third party

Means 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 controller or the processor, is authorized to process the data.

2.14 Recipient

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

2.15 Informed consent

Means 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.

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 on cancer determinants, exposure to carcinogens and effects of interventions in prevention and early diagnosis, provided that patients can be identified and linked individually to other files. The cancer registry has in many countries also proved to be an important tool for evaluating and planning health services, in addition to research; again preferably if data can be linked to other files, for example, from the hospital and the clinicians involved with the case.

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.

In some countries, the storage and use of personal data on cancer patients require informed consent of the data subject. However, the European Directive 95/46/EC on the protection of individual's rights makes exemption for processing done to comply with a legal obligation (Article 7), or when data are required for preventive medicine (Article 8.3). In the same Directive it is explicitly stated (Article 6) that personal data must be processed fairly and lawfully, collected for specified purposes, be adequate and relevant for the purpose, be accurate, complete and kept up to date, and not kept identifiable longer than necessary for those purposes. Data for historical, statistical and scientific purposes may be processed further (e.g. data linkages), and stored for longer periods, provided the Member State provides appropriate safeguards. Such safeguards need not be of a technical nature, including complicated organizational and computerized procedures, but may be of a legal nature, with supervisory bodies controlling data use and registry procedures as seen in the Nordic countries with data inspection agencies.

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 on cancer patients.

Fulfilling the legal requirement to 'report' can mean simply allowing access for registry staff to abstract specified information (so-called active cancer registration). It may require, on the other hand, provision of copies of various documents from the patient records, on special notification forms, or electronic notification either by a dedicated electronic form or by extracting already computerized information.

If the registration is based on data linkage of one or more patient-related registries, vital statistics registries, and population registries, legal provision must be in place for the use of such registries for this purpose, and for the data items that may be transferred to the cancer registry. Usually this should be stated in the by-laws of the registries in question, as well as in the cancer registry by-laws.

3.3 Sources of information

Registries should restrict themselves to the collection of the most important data, of a high quality and completeness (Jensen *et al*., 1991), and ensure they can link to other databases for various other data items when necessary.

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, increasingly, on magnetic media, or may be derived from computerized 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 comes 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 (residence). 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 (Directive 95/46/EC Article 6) and collect data that are adequate, relevant and not excessive in relation to the 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 more chance of an unintended breach of confidentiality when releasing data).

The data items in the recommended minimum data-set for cancer registries are listed in Table 1.

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 research intended to advance the understanding of the causes, occurrence and outcome of cancer. However, there is a distinction between clinical use and research in the Directive. Clinical use requires that the data subject be informed about processing, and the subject has the right to obtain information about him or herself from the controller. This is not the case if the cancer registry is using the collected data solely for scientific research or statistical purposes (Articles 11, 12 and 13.2).

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

3.5.1 Quality of diagnosis, treatment and health care

The clinical use of identifiable data relating to patients registered with cancer arises in 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 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, provided this purpose is included in the registry by-laws. Identification of the person is indispensable for these tasks. It is pertinent that the registry and the physician observe the

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	

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 specialized 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 research

(*a*) *Studies of 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, computerized or both, and whereas linkage always requires knowledge of the identity of individuals with cancer, irrespective of whether the ID information appears in encrypted form or not (see 5.8.1), the resulting publications always present anonymous or aggregated data. It is, however, pertinent for the quality control in such studies that the researcher has the possibility to check the quality of the linkage procedures manually and sort out spurious findings, and for these purposes identifiable data must be available. The credibility of studies in which such quality control cannot be performed is low, and results in the worst-case scenario can be misleading.

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. It must be observed, however, that contact with the data subjects should be undertaken through the treating physician or hospital, and with the approval of ethical committees in place in the country.

(*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 or breast, develops less frequently and mortality decreases in a screened population or subgroup. This requires the comparison of lists of individuals with cancer detected by the screening programme with cancer registry files. The cancer registry may thus be essential for adequate evaluation of a population-based cancer screening programme, providing the information is not available in any other way.

(*c*) *Evaluation of survival from cancer*

By matching death certificates to cancer notifications received by the registry, it is possible to assess the survival of all persons with cancer in a defined population. Survival from cancer in the population as a whole is frequently quite different from that reported for selected series of patients (e.g. in 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 for a given cancer by the extent of spread at diagnosis, or by the type of treatment. This type of research is possible only if the registry can link identifiable cancer registrations with death certificates; such evaluation of cancer survival is now routine practice in many registries.

3.5.4 Genetic counselling

The use of data in cancer registries on families for genetic counselling of individuals concerned about a possible heritable cancer disease is tempting, because of the completeness of cancer registries and the fact that all the necessary data are available in the registry (cancer type, sex, age of family member at cancer

and/or death). Such use is, however, not compatible with Article 7 of the Directive, because the counselling cannot be considered of 'public interest' [although inaccurate counselling may lead to overestimation of risks and unwarranted consequences, e.g. prophylactic mastectomy], nor are such activities included in Article 8 under medical diagnosis and preventive medicine. Therefore the use of registries for genetic counselling can only be on the basis of the informed consent principle. The policy below was developed by the United Kingdom Association of Cancer Registries:

"(i) Request 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 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, when possible, the GP 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 of hospital of managing consultants and (for living patients) name and address of GP."

The medical practitioner, or other recipient of the data responsible for the request, should sign a declaration to the effect that he or she has understood and agrees to act in accordance with the policy statement.

3.5.5 Use of aggregate data

(*a*) *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, etc. 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 after the compilation of the data-set during which data are identifiable.

(*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 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 customarily 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 unauthorized 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 confidential 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 confidentiality and to make good 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 and cancer research. It is important to observe that confidentiality rules follow the intention laid down in the Directive 95/46/EC, and are not so strict that the rules will hinder usage of the data, which again is described in the aims of the registry.

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 and those notifying them (data subjects and data suppliers), to include identifiable data 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 or for research projects.

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. For deceased persons, as for live, information on data disclosure is exempt based on article 11.2. A supervisory regulatory body may provide sufficient safeguards against breaches of confidentiality for deceased persons.

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, image scanned records 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.

Precautions should be taken when maintaining electronic files, and the transmission of confidential data by means of the Internet or via e-mail 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. One basic principle is, as in the European Directive, informed consent. This principle cannot be followed for successful cancer registration and the European Directive exempts cancer registration from informed consent (1.3.2).

5. Measures for data confidentiality

5.1 Responsibility

The Director of the cancer registry is usually in legal terms the 'controller' or the 'processor' (Directive 95/46/EC, Articles 2(d) and 2(e)) responsible for maintaining the confidentiality of identifiable data. The Director must ensure that the registry staff and 'third parties' 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. 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 there should be an adequate system of computerized security measures (see section 5.8.1). Further fulfilment of the conditions for released data should be followed by the Director (see section 6). The specific criteria for the Director's nomination (responsibility for data privacy and security) may be designated by law. If not, the criteria should be detailed in the Director's job description, and failure to comply will be considered a breach of the oath of secrecy (see section 5.2).

5.2 Oath of secrecy

Duly trained and specialized staff should be appointed to run the cancer registry in accordance with its aims and rules of operation. It is recommended that, as part of their contract of employment or conditions of service, each member of the registry staff be required to sign a special 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 unauthorized 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. Furthermore, it should be made clear that a dismissal on these grounds will be disclosed to employers within the health sector if so requested, thereby making the oath of secrecy comparable to the professional medical oath of secrecy. 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

Unauthorized access should be prevented. Physical access to the registry premises has to be restricted 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 authorized to enter the registry.

5.5 Active registration

Registry staff assigned to collect information at source (active registration) 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), 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, and where possible, changes in personnel should be notified to these sources in advance.

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) (Directive 95/46/EC, Articles 2(d) and 2(e)).

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 ID information should be mailed separately from the health information, to be combined using an internal code number by authorized staff upon receipt of both mailings.

For data on electronic media, the encryption of ID information with a special key is an alternative to the procedure of two separate mailings (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 unauthorized personnel.

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

5.6.2 Magnetic or electronic data transmission

When identifiable data are sent electronically by magnetic or other machine-readable form, 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 unauthorized person, measures to check for incorrect or corrupt files must also be taken (Directive 95/46/EC Article 17). Among the precautions that might be taken are:

(a) Encrypting of names and other ID information at various levels of complexity, with a special key available only to authorized 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) Including tabulations and counts by which the content of the transferred data can be checked, and 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 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 measure complies with the national law (Directive 95/46/EC Article 4). Transmission should be in accordance with the above procedures.

Any unnecessary transfer of identifiable data outside the registry should be avoided. Alternatively, data may be provided with a key for identifying individuals and the key kept at the cancer registry.

5.7 Use of telephone

It must be clearly recognized 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, nor should the registry staff seek information in this way.

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 a call-back procedure followed, using only officially published telephone numbers.

5.8 Use of computer

Physical and electronic measures should be used to prevent unauthorized access to information held on the computer. Electronic measures are subject to rapid evolution, and better 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 be used that do not appear on the screen when typed.

(c) Passwords should be changed at intervals, and minimum requirements for changes (interval and password) stated 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 authorized users.

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

(f) Sessions which have been inactive for more than 10 minutes should be automatically closed, and instructions given to staff to close sessions immediately after use.

Encryption of data has been proposed for preserving confidentiality in storage and communication of confidential data (Anderson, 1995).

The matching and linking of encrypted individuals however need great care, as also errors may be encrypted. Only limited experience exists with these methods in cancer registries. So far fully functioning systems have not been developed.

One other method to increase the difficulty of unauthorized use is the separation of the identity information and the cancer data. The computer of the cancer registry may be kept in complete isolation from the rest of the computer world. One-way traffic of data may be controlled with a specific security program, the so-called firewall.

All testing of new hardware and software should be carried out with special test data. Hard disks, floppy disks and tapes must be efficiently erased or destroyed when taken out of use.

Technical measures administered for the sake of data protection should not lead to a compromise in 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 anonymized data should be utilized. 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 and its changes should be made frequently and regularly as a protection to avoid the loss of the database, and should be stored in a physically separate, safe location.

5.9 Unauthorized access to computer system

It must be recognized 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 into such systems should at least be capable of foiling casual attempts to gain unauthorized 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 preferable 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 image scanned to 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 and research purposes, in line with the code of good conduct of the International Epidemiological Association for other research data. The storage of records on paper should be reduced to a minimum for both confidentiality and practical reasons. Paper records or copies thereof (irrespective of media) are accessible to casual inspection, and require no special expertise to gain access. Image scanned files which may be password protected are thus an exception. Specific measures for 'paper records' that may be considered include:

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

(b) Defining which members of staff have access to the room where these 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 authorized to do so (e.g. cleaning personnel) are not able to scrutinize 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 specialized and officially authorized services for the safe disposal of confidential waste.

5.12 Review of confidentiality and security procedures

It is recommended that cancer registries undertake formal review of their security procedures annually, and at the same occasion revise access files and logs. It may be helpful at five-year intervals to recruit the services of specialist advisers to ensure that the registry's procedures for the maintenance of confidentiality are up to date, and cover all aspects of the registry's operations.

6. Release of data

The release of aggregate data, in tabular or equivalent formats, and anonymized data does not breach confidentiality. However, care should be taken that an individual may not potentially be identified from such data, e.g. by date of birth (age), sex, and residence in a small geographical area. As a general rule, only

data specifically needed for the question raised should be released.

Many of the uses of registry data, both in health care planning and in research, involve the release of identifiable data on individuals registered with cancer. The derogations to the European Directive 95/46/EC (Articles 8.3 and 8.4, and further explained in recital 34 of the Directive) can be applied in order to legalize the use and the release of data for preventive medicine, including 'public health purposes and scientific research'. National legislation may in the public interest add further exemptions by law or legal order.

Furthermore, the Directive 95/46/EC (Article 11.1) specifies the need to inform the data subject about the disclosure of data to a third party at the time when data are disclosed. The registries have, however, derogation in Article 11.2 when the processing is for statistical, historical or scientific research, and the provision of information is impossible (deceased persons) or involves a disproportionate effort or national law allows the disclosure. Member states shall in these cases provide appropriate safeguards that must be observed by registries.

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) ensures that the law and national guidelines are followed and confidentiality is preserved when data are released. The research projects for which the data are to be released should be scientifically sound. A mechanism to decide about what can be regarded as sound should be established. The director, a scientific committee or an authority could be made responsible for that decision.

6.2 Limitations on data release

(a) National legislation with respect to data confidentiality, patients' rights etc. 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 asked 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 patient registered with cancer should be given to the treating physician, subject to the legislation concerning the transfer and release of medical (clinical) data in the country.

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

The registry should prepare a public, written document that sets out the criteria and procedures applicable to the release of its data, particularly the release of identifiable data for research. This document could be provided to researchers requesting identifiable data, and reference made to any national legal and ethical requirements.

A request for the release of confidential data should be made in writing to the supervising authority (an example form is attached, see Appendix 1). The release should fall within the accepted uses of registry data and the requirements for safeguarding the confidentiality of the data.

6.4.1 The request should include*:*

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

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

(c) The name and position of the person in charge of the data after their release.

(d) The name and position of other persons who will have access to the data after their release.

(e) The period of time for which the data would be used, the way the data would be handled and the way in which the data (with all its copies) would be disposed of, returned or destroyed after this period has elapsed.

6.4.2 The requesting party should also give an assurance to the cancer registry director or the body in charge of data release, by verified signature, that the intended recipient of the identifiable data will:

(a) Observe the same principles and obey the same laws as are observed and obeyed by the staff of the cancer registry.

(b) 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.

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

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

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

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

(g) Give due acknowledgement to the registry for provision of the data.

(h) Provide the registry with a copy of all published and pertinent results when accepted for publication or, if not published, at the time of disposal of the data.

6.5 Provision of data to individuals

The code of confidentiality for cancer registries (IARC/IACR Guidelines on Confidentiality in the Cancer Registry, 1992) advises that registries should not generally inform individuals whether or not there are data about them held in the registry, but 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.

Unless a national law explicitly exempts the controller from releasing information to the data subject, or the data are being processed solely for scientific research (Directive 95/46/EC Article 13), registries are obliged, upon request at reasonable intervals, without excessive delay and expense, to inform a data subject whether or not data relating to him or her are in the cancer registry. The information should contain the purpose, the categories of data (variables) and categories of the recipients of the data (Directive 95/46/EC Article 12).

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

One of the reasons for the European Directive 95/46/EC is the expected increase in scientific and technical cooperation (recital 6). The Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data regulates the cross-border flow of data in a consistent manner, and safeguards the fundamental rights of individuals. Furthermore, the Directive should lead to an approximation of national laws, and secure a similar and higher level of protection for the rights and freedoms of individuals, and in particular the right to privacy. Within the European Union the processing of personal data is governed by the laws of the member state in which the data is processed (machines, software). In

principle personal data can be transferred, but this should be done only when necessary. When the study design requires that identifiable data be transmitted across registry or national borders, and if national legislation permits and the level of protection satisfies Article 25 of the Directive, then such data can be transferred. The data should at least 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 seek approval for the transfer with national authorities.

The transfer of personal data to third countries (Article 25) is also allowed if the country complies with the national provisions for confidentiality and the European Directive, and if the country in question can afford an adequate level of protection, which has been assessed by a member state of the European Union. A derogation (Article 26.1(d)) from these requirements can be made if the transfer is necessary on important public interest grounds.

Research projects involving the provision of data about individuals from many cancer registries, sometimes in different countries, have provided valuable information about cancer risk. 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 within the study. This number can then be used instead of the subject's identity in data files contributed to the study coordinating centre. It should, however, be observed that the data in legal terms are still personal and identifiable.

6.7 News media

Cancer registries are frequently approached by the press for information on cancer. It is recommended that all such enquiries be referred to the Director or other nominated staff member, to whom specific responsibility for dealing with the press has been delegated.

Great care should be taken not to disclose any personal data, or data that by linkage to other data may disclose the identity of individuals (such as sex, age, small area) to the media.

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 the national or regional archives regulated by law be identified, in advance, to store the registry archive, a registry description including 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 for a minimum of 50 years. The 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, R.J. (1995) Security in clinical information systems. University of Cambridge (internet URL http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html)

Coleman, M.P., Muir, C.S.. & Ménégoz, F. (1992) Confidentiality in the cancer registry. *Br. J. Cancer*, **66**, 1138–1149

Cordier, L.J. 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 1995; 5–7

Directive 95/46/EC of the European Parliament and of the Council of 24 October 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* 1995; 281(1):31–50

Fritz, A., Percy, C., Jack, A., Shanmugaratnam, K., Sobin, L., Parkin, D.M., 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. IARC Internal Report no. 92/003. IARC, Lyon, 1992

Jensen, O.M., Parkin, D.M., MacLennan, R., Muir, C.S. & Skeet, R.G. (eds) (1991) *Cancer Registration – Principles and Methods* (IARC Scientific Publications No. 95), Lyon, IARC

Medical Research Council (1985) Responsibility in the use of personal medical information for research: principles and guide to practice. *BMJ*, 290, 1120–1124

Muir, C.S., Démaret, E. & Boyle, P. (1985) The cancer registry in cancer control: an overview. In: Parkin D.M., Wagner, G. & Muir, C.S. (eds), *The Role of the Registry in Cancer Control* (IARC Scientific Publications No. 66), Lyon, IARC, 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

Annex 1. Example of application/release form

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 (SAME DETAILS AS IN POINT 3)
5. VENUE FOR THE PROJECT
6. CONTACT PERSON (NAME, ADDRESS, PHONE, FAX, E-MAIL)
7. TYPE OF PROJECT
   - DURATION (BEGINNING, END)
   - DEFINITION OF THE DATA ITEMS REQUESTED FROM THE CANCER REGISTRY
   - OTHER DATA MATERIALS TO BE USED, THEIR WAY OF USE AND PERMISSION RECEIVED OR (TO BE) 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
11. ASSURANCE

I agree to handle the data according to the terms included in Appendix A.

Date, signature

Person in charge of the project

Date, signature

Other persons with access to the data to be released

Date, signature

Documents to be appended to application/release form:
Appendix A. Terms for use of the data (see below)
Appendix B. Project plan
Appendix C. Other permissions received
Appendix D. Ethical committee's statement
Appendix E. A short CV of the person in charge

Appendix A. Terms for use of the data (sample):

1. The data may only be used for the purpose specified in the project plan.

2. The data may not be released further 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.

Annex 2 Sample oath of secrecy

Confidentiality agreement

Declaration of confidentiality
Permanent staff

Name: _____

All the data collected and held by the Thames Cancer Registry are confidential data relating to identified individuals. The manual and computer files are registered under the Data Protection Act 1998. Data are not to be accessed, disclosed, published or communicated in any way other than as provided for in the Registry's standing instructions on security of information, computer systems and premises.

All Registry staff also have a duty to preserve the confidentiality of anything of a confidential nature seen or heard in the course of their work during and after their employment at the Registry. **This includes not discussing cases that you have seen during your work. For example if you have seen a case for a famous person, those details are confidentional and should not be discussed with family, friends, neighbours etc.**

All Registry staff have a duty to know the standing instructions on security and comply with them. In case of doubt staff are required to consult their department manager.

To be signed by the member of staff:

I have read the above declaration and understand that any breach of confidentiality may result in disciplinary action, which may extend to dismissal.

Signed: _____

Dated: _____