



# **Guidelines on Confidentiality and ethics for population-based cancer registration and linked activities in Europe**

European Network of Cancer Registries

International Agency for Research on Cancer

**Version 3, May 2011**

## European Network of Cancer Registries Working Group on Confidentiality

The Steering Committee of the European Network of Cancer Registries (ENCR) has decided to update the guidelines on confidentiality in cancer registries. The last version was published in 2002<sup>1</sup>, three years before the endorsement by the European Parliament and Council of the European Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data<sup>2</sup>. The European Directive is exhaustive, and is used as an example in many countries. This revision may also have value outside the European Union (EU). The EU Directive defines the levels of protection for data on individuals and national legislation may further specify these.

The need to revise the guidelines on confidentiality was identified in a European survey of cancer registries<sup>3</sup>. A need to expand the guidelines to include ethics and linkages to other databases was also identified. A Working Group was formed including specialists in epidemiology, screening, biobanks and clinical databases, under the auspices of the EUROCOURSE project.

The terms of reference were:

- (a) To update the Guidelines on Confidentiality in the Cancer Registry published by the European Network of Cancer Registries in 2002
- (b) To include ethics and linkages to other databases.
- (c) To examine to what extent these guidelines could be used in cancer registries outside Europe, and to identify areas in the guidelines where difficulties may arise.

The members of the Working Group were:

Hans H. Storm, Denmark (Chairman)  
Emanuele Crocetti, Italy  
Timo Hakulinen, Finland  
Alexander Katalinic, Germany  
David Brewster, Scotland  
Michel Coleman, England  
David Forman, IARC  
Mati Rahu, Estonia  
Marc Arbyn, Belgium  
Laufey Tryggvadottir, Iceland  
Sven Törnberg, Sweden  
Evert-Ben van Veen, Holland

Secretariat:

Mikkel Hyldebrandt Jensen, Danish Cancer Society  
Lone Rosander Thomsen, Danish Cancer Society  
Birgitte Ødegaard, Danish Cancer Society

The Working Group met in Copenhagen and in Lyon to review the guidelines in the light of the European Directive.

Agreement was reached on the changes required in the light of developments in the law, ethical standards, technology, record linkage and cancer registration methods.

We are grateful to all the registries that readily sent copies of the confidentiality rules and codes of conduct from their area or from registry associations in their country. Each member of the Working Group took responsibility for editing sections of the guidelines. The final version was agreed by all members of the Working Group, accepted by the Steering Committee of the ENCR and released in November 2011.

Hans H. Storm

Chairman, Working Group on Confidentiality of the European Network of Cancer Registries in the framework of the EUROCOURSE project.

## TABLE OF CONTENTS

Summary of conclusions and recommendations	7
A. Principles of confidentiality and the role of the cancer registry .....	7
B. Measures for data confidentiality, protection and security .....	7
C. Release and use of registry data .....	8
1. Purpose of guidelines on confidentiality and ethics in the cancer registry	10
1.1 Background .....	10
1.2 Aims .....	10
1.3 European Directive on Data Protection (95/46/EC).....	11
1.3.1 Privacy .....	11
1.3.2 Informed consent.....	11
1.3.3 Derogation to the requirement for informed consent .....	11
1.3.4 Derogation to the obligation to inform subjects about data processing .....	12
1.3.5 Clinical use of data.....	12
1.4 Use of guidelines.....	12
2. Definitions	12
2.1 Cancer .....	12
2.2 Cancer registration .....	13
2.3 Cancer registry .....	13
2.3.1 Hospital-based cancer registries.....	13
2.3.2 Population-based cancer registries.....	13
2.3.3 General cancer registry .....	13
2.3.4 Specialised cancer registry .....	13
2.4 Data subject.....	13
2.5 Confidential data (personal data) .....	13
2.6 Treating physician.....	14
2.7 Security .....	14
2.8 Data protection.....	14
2.9 Processing of personal data (European Directive definition).....	14
2.10 Controller .....	15
2.11 Processor .....	15
2.12 Third party .....	15
2.13 Recipient .....	15
2.14 Informed consent .....	15
2.15 Ethical standards .....	15
3. Role of the cancer registry	15
3.1 Function of the cancer registry.....	15
3.2 Legal basis of registration .....	16
3.3 Sources of information.....	16
3.4 Data items .....	17
3.5 Use of cancer registry data.....	18
3.5.1 Quality of diagnosis, treatment and health care .....	18

3.5.2	Transfer of identifiable data for registration purposes .....	18
3.5.3	Use of identifiable data for cancer control and research .....	18
(a)	Studies of the causes of cancer .....	18
(b)	Evaluation of screening .....	19
(c)	Evaluation of survival from cancer .....	19
3.5.4	Genetic counselling .....	19
3.5.5	Use of aggregate data .....	20
(a)	Research and public health surveillance .....	20
(b)	Health care planning .....	20
4.	Principles of confidentiality .....	20
4.1	Underlying concept of medical confidentiality .....	20
4.2	Sharing of confidential clinical information .....	21
4.3	Legal protection of data suppliers .....	21
4.4	Confidentiality and utility .....	21
4.5	Scope of confidentiality measures .....	21
4.6	Confidentiality of data on deceased persons .....	21
4.7	Indirectly identifiable data .....	22
4.8	Methods of data storage and transmission .....	22
4.9	Ethics .....	22
5.	Measures for data confidentiality and security .....	22
5.1	Responsibility .....	22
5.2	Oath of secrecy .....	22
5.3	Display of reminders .....	23
5.4	Physical access to the registry .....	23
5.5	Active registration .....	23
5.6	Transmission of information .....	23
5.6.1	Postal and courier services .....	23
5.6.2	Electronic data transmission .....	24
5.6.3	Processing and matching of data by external agencies .....	24
5.7	Use of telephone and fax .....	25
5.8	Use of computer .....	25
5.8.1	Access to data .....	25
5.8.2	Demonstrations .....	26
5.8.3	Back-up .....	26
5.9	Unauthorised access to computer system .....	26
5.10	Storage of original data .....	26
5.11	Disposal of physical records .....	27
5.12	Review of confidentiality and security procedures .....	27
6.	Release of data .....	27
6.1	Responsibility for data release .....	28
6.2	Limitations on data release .....	28
6.3	Release of identifiable data for clinical purposes .....	28
6.4	Release of identifiable data for scientific and cancer control purposes .....	28
6.5	Provision of data to individuals .....	29
6.6	Transfer of data across borders .....	30
6.7	News media .....	30

6.8 Cessation of cancer registration .....	30
REFERENCES	32
APPENDIX	33

## 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 and ethics as customarily apply to the doctor-patient relationship; this obligation extends indefinitely, even after the death of the patient (sections 4.1, 4.6 and 4.9).
- 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 unauthorised 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 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 and fax 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 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 audit trails and 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 and other 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 and use of registry data**

- C.1 Appropriate use and release of cancer registry data is central to the utility of the registry. The data may be used by the registry and other bodies for a variety of purposes including cancer research, health care planning, public health surveillance, and the monitoring and evaluation of interventions. The registry should develop suitable procedures for use and release of data that ensure the maintenance of confidentiality and ethical standards (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, ethical standards and the registry's guidelines on confidentiality and ethics. Also the scientific soundness of the project should be judged (section 6.1).



- C.3 National legislation with respect to confidential data should be observed. As a general rule, 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).
- 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 Provision of own data to the data subject must be given 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 and ethics in the cancer registry

## 1.1 Background

These guidelines for confidentiality and ethics in population-based cancer registries in Europe build upon the European guidelines published in 2002<sup>1</sup>. They are also consistent with the guidelines first published by the International Association of Cancer Registries in 1992<sup>2,3</sup> and revised in 2004<sup>4</sup>. In brief, the code of confidentiality for cancer registries defines the measures to be taken to protect the privacy of the individual patient, the doctor and the hospital. They specify what information should be regarded as confidential, and set out measures for establishment and periodic review of both physical and electronic security procedures, the requirements to be met before release of confidential data for research and other purposes, and the constraints to be satisfied by any publication derived from the data.

At the same time it is increasingly being recognised that the ethical standards which apply to epidemiological research need to be different from those applying to clinical research on individual patients. Although there may be a need to access and/or link individual and personal data, these details are not disclosed, as the fundamental nature of epidemiology is group-based statistics<sup>5,6</sup>.

These guidelines are also designed to be 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<sup>7</sup>. That Directive provides the basis for national legislation in EU Member States for the protection of individuals with regard to the processing of personal data.

Cancer registration procedures have been modified in many countries, moving from paper-based systems to systems largely based on computerised data capture and storage<sup>8</sup>. New information technology promises to make accurate information more readily available at a lower cost, but it raises concerns from the point of view of confidentiality, because of the easy storage and dissemination of huge volumes of data. Despite these concerns, there is evidence of strong public support for cancer registration and the use of the data for research<sup>9</sup>. These concerns and recommendations related to the protection of electronic health information have been dealt with by various committees<sup>10,11,12,13</sup>.

The main objective of guidelines for confidentiality was outlined<sup>14</sup>: (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; (c) and 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

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

- a) The definition of terms for cancer registration and confidentiality, with reference to the European Directive
- b) The articles in the Directive that are of particular 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 ethical standards, for the use and release of registry data in accordance with these principles

### 1.3 European Directive on Data Protection (95/46/EC)<sup>7</sup>

#### 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.

#### 1.3.2 Explicit consent

Article 7 of the Directive indicates that unambiguous consent is needed for the use of identifiable data about persons, unless that use is required by the vital interests or contractual obligations of the data subject, or by legal obligations of the data controller, or in the public interest. Article 8 prohibits the processing of data concerning health, unless explicit consent is given or other conditions apply see below 1.3.3. Many uses of registry data, however, both in health care planning and in research, involve the release of identifiable data about individuals registered with cancer.

If there were no derogations to the principle of explicit consent (see below), the principle would make it virtually impossible to use data from a cancer registry, for these reasons:

- a) Studies based on cancer registry data often involve hundreds of thousands of cancer patients, and contacting every patient would be impossible, especially as in many studies a large proportion would already be deceased. The practical burden of seeking consent in this context would therefore be disproportionate.
- b) The repeated burden for patients or their relatives of being asked to consent to the use of their data for research is of concern.
- c) Seeking general consent for whatever scientific or statistical use might be made of the cancer registration data in the future would impose unacceptable work load on medical personnel and would lead to unacceptably low completeness of cancer registration<sup>7</sup>.
- d) From a legal point of view, consent only remains valid for a limited period of time, whereas it is not possible to foresee all the research questions that may arise in the future.
- e) Incompleteness of registration would vary between registries as a result of differences in the manner in which consent is sought or given. This would invalidate international comparisons of cancer incidence.

#### 1.3.3 Derogation to the requirement for explicit consent

Article 8(3) of the Directive exempts data collection from the requirement for the patient's consent if it is: "... required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy." This derogation includes all the components

required for cancer registration and most uses of cancer registry data for research. National legislation may add further exemptions or restrictions by law or legal order. These do not override the requirement for data processing to be ‘fair and lawful’ under the Directive.

#### *1.3.4 Derogation to the obligation to inform subjects about data processing*

Article 11.1 of the Directive specifies the need to inform the data subject about the disclosure of data to a third party when data are disclosed. The registries, however, fall under the derogation in Article 11.2 when processing is for statistical, historical or scientific research, or the subjects cannot be informed (deceased persons), or provision of information would involve 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. EU Member States are required to provide appropriate safeguards that must be observed by registries.

#### *1.3.5 Clinical use of data*

Data release and use for clinical and screening purposes may be included in the function of some cancer registries. These data will usually be supplied to the treating physician or screening organisation and used for the benefit of the individual with their informed consent. Such release and use must still be subject to the applicable legislation. Information leaflets in screening programmes should inform individuals that their data may be used for quality control and research.

### **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. The data controller has an obligation to ensure that the registry data meet these standards of quality. 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 modification to conform to national legislation. Rather, they are intended to present the basic principles of confidentiality set out in the European Directive, 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 continue to be kept under review by the ENCR, and further 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<sup>15</sup>. Cancer registries always record invasive malignant neoplasms, but many also record *in situ* carcinomas (e.g. cervix, breast, bladder), neoplasms of uncertain behaviour and benign tumours (e.g. brain).

## 2.2 Cancer registration

Cancer registration is the process of the continuing, systematic collection of data on the characteristics of the neoplasm, the person, the treatment and the outcome, for all persons diagnosed with cancer. It is the basic activity of a cancer registry.

## 2.3 Cancer registry

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

### 2.3.1 Hospital-based cancer registries

Cancer registries that aim to record information on all cancer patients seen in a given hospital or group of hospitals, irrespective of geographical areas, are said to be hospital-based.

### 2.3.2 Population-based cancer registries

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.

### 2.3.3 General cancer registry

A cancer registry may be described as general if all malignant neoplasms are registered.

### 2.3.4 Specialised cancer registry

A cancer registry may be described as specialised if registration is restricted to neoplasms of a specific type (e.g. breast cancer, haematological malignancies) or age group (childhood cancers).

## 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 that could in theory permit the identification of an individual patient's (data subject) health data 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 from a reference number or other identifying information such as names, date of birth, etc., or to factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

However, the collection of unambiguous identifying information on the data subject is necessary, both in order to maintain the quality of the data and for use of the data for research and public health. Anonymisation if used must be two-ways, enabling the registry to consult the source data to rectify mistakes or errors. The following list provides some examples:

- a) To avoid duplicate registration of patients visiting more than one healthcare institution
- b) To study cancer survival as a measure of the effectiveness of cancer services; this requires linkage of cancer registration with the death registration, which may arise decades after the cancer diagnosis
- c) To study geographical clusters of disease (high-risk areas)
- d) To study the family history of disease, in order to give appropriate advice about familial or genetic risks
- e) To study the late effects of occupational exposures or cancer treatment, by linkage to other health records, sometimes many years after diagnosis and treatment of the cancer.

The dates of birth, diagnosis and death are needed for many research purposes. The data items considered confidential combined with the health data, either alone or in combination with other data items (x), are listed below:

- a) Names
- b) Unique reference number (e.g. national identity number)
- 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 the data items in d) or e)

In many instances, the combination of age, sex, year of diagnosis and small area code may be regarded as confidential because a person could be identifiable if the population in the area is sufficiently small. Release of such data should be strictly controlled.

## 2.6 Treating physician

The treating physician is the doctor responsible for the patient's treatment: either the primary care physician (general practitioner or GP), or the doctor 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 at which 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 unauthorised access to the registry's data, irrespective of the medium in which they are stored or transmitted.

## 2.8 Data protection

Data protection includes both prevention of physical access to the data (security), and protection of the data to avoid corruption during many years of storage. Backup procedures for electronic media are also required. The term should in this context not be confused with confidentiality (privacy), the aim of which is to protect the individual from unauthorised disclosure of data.

## 2.9 Processing of personal data (European Directive definition)

This denotes any operation or set of operations including data linkages 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.

## **2.10 Controller**

Denotes the natural or legal person (in this context, usually the 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 law or regulation, the controller or the specific criteria for his or her nomination may be designated by law.

## **2.11 Processor**

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

## **2.12 Third party**

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

## **2.13 Recipient**

In this context, a 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.

## **2.14 Explicit consent**

Explicit consent means any freely given specific and informed decision of the data subject by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

## **2.15 Ethical standards**

In the context of these guidelines, ethical standards mean the standards applied to population-based and epidemiological research, which differ from the standards applied to the individual doctor-patient relationship, but adhere to the standards of the International Epidemiology Association. (Good Epidemiological Practice. IEA guidelines for proper conduct in epidemiologic research. November 2007)<sup>16</sup>.

# **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<sup>17</sup>, 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 enable 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 provided that patients can be



identified and linked individually to other files, e.g. exposure to carcinogens, biobanks, screening records, employment records, etc. 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 explicit 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. Non sensitive personal 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 organisational and computerised 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. For sensitive data, as stored in cancer registries this can be done in accordance with Articles 8.3 and 8.4.

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 computerised 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<sup>14</sup>, 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, as electronic records, 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 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 (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 (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 suggested minimum dataset for cancer registries are listed in Table 1.

**Table 1.** Items of information collected by registries<sup>14</sup>

<b>Essential variables</b>	
Personal identification	Names (in full) AND/OR unique personal identification number
Sex	Male or female
Date of birth	Day, month, and 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	
<b>Recommended variables</b>	
Date of last contact	At least month and year
Status at last contact	(At least dead or alive)
Method of first detection	
Stage or extent of disease	
Initial treatment	

### 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 for cancer control<sup>18</sup>. The data are used 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 information to the data subject about processing, and gives the data subject 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 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 cancer control and research*

##### (a) Studies of the causes of cancer

Case-control and cohort studies help 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 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 the programme is achieving its goals. In comparison with an unscreened population, screening for pre-cancerous lesions of the cervix should decrease the incidence of cervix cancer, whereas screening for breast cancer should increase the incidence of early cancer and decrease mortality. The cancer registry enables the identification of interval cancers, thus the efficiency of the programme is monitored. This requires the comparison of lists of individuals with cancer detected by the screening programme with cancer registry files. The cancer registry is thus essential for adequate evaluation of a population-based cancer screening programme.

#### (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 only possible 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 hereditary cancer disease is tempting, because of the completeness of cancer registries and the fact that all the necessary data is available in the registry (cancer type, sex, age of family member at cancer and/or death). Such use is, however, not readily possible following 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, as far as living relatives are concerned, 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 and public health surveillance

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 dataset 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 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 nonmedical, technical and clerical, who provide services and manage the health care institutions’<sup>19</sup>. Despite this essential dispersion of confidential information within the clinical team, the ultimate responsibility for the maintenance of confidentiality in the clinical setting remains with the treating physician. Therefore, as well as the patient, the treating physician who provides information to a cancer registry 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 ethics, and that data of high quality are being collected and used for the benefit of cancer patients, cancer control 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 linkage and 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, screening databases, biobanks, 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 by other means, and their transport or transmission by registry personnel in any format. The procedures involved may differ, but the underlying principle is the same. The transmission of confidential data by means of electronic media, 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. The Helsinki Declaration is primarily aimed at protecting individuals subject to invasive, intrusive or potentially harmful interventions. Research ethics committees should enable high quality epidemiological research of benefit to public health. Ethical evaluation criteria must be appropriate to the type of study (IEA guidelines). For example, the basic principle of informed consent, as set out in the European Data Protection Directive, cannot be followed for successful cancer registration and large data linkages. It should be noted that the Directive exempts cancer registration and public health research from the requirement for explicit consent (1.3.2).

### **5. Measures for data confidentiality and security**

#### **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 an adequate system of computerised 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 specialised 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 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. 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**

Unauthorised 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 authorised 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 backup 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 authorised staff upon receipt of both mailings.

For data on electronic media (e.g. CD, DVD, memory sticks), 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 unauthorised personnel.

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

### 5.6.2 *Electronic data transmission*

When identifiable data are sent electronically, 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 (Directive 95/46/EC Article 17). Among the precautions that might be taken are:

- (a) Ensuring that the address of the recipient is correct. The risk of sending to the wrong recipient may be reduced by using different media for contact before sending any data or ID key.
- (b) Encrypting of names and other ID information at various levels of complexity, with a special key only available to authorised users (see also section 5.8.1).
- (c) Sending data files, the identifiable data should be sent separately from the other data, using a link number to enable the reconstitution of the record by the intended recipient. This may also be achieved by using different media for ID and data files.
- (d) Transmitting data can be achieved by download of data through a secured, encrypted FTP (file transfer protocol) where the access code and instructions are transmitted in accordance with (a).
- (e) 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.
- (f) Requesting the recipient to confirm safe receipt of the data and their integrity

### 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 (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 and fax

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 or by fax by registry staff, nor should the registry staff seek information in this way. If a fax is used, it should be a “safe haven” fax. The fax number should be checked carefully before transmission.

The need for the registry to pass identifiable information to external callers by telephone should be infrequent. Registry staff should be alert to attempts to access patient information fraudulently. 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 unauthorised access to information held on the computer. 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.

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) Passwords should be sufficiently complex and should not appear on the screen when typed. Automatic storage of passwords linked to user name should be disabled.
- (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 (audit trail) should be kept by the computer of all successful and unsuccessful attempts to enter the system, and session activity by authorised users. The Director should authorise a limited number of persons to have access to the audit trail.
- (e) Different levels of access to the database, supported by password protection and user recognition, should be defined, so that only users authorised 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.
- (g) The computers of the cancer registry should be in one environment protected by a firewall.
- (h) Encryption of data has been proposed for preserving confidentiality in storage and communication of confidential data<sup>20</sup>.

The matching and linking of encrypted individuals however need great care, as errors may also 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 unauthorised use is the separation of the identity information and the cancer data.

- (i) All testing of new hardware and software should be carried out with special test data. Electronic storage media must be efficiently erased or destroyed when taken out of use.

### 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 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, secure location, ideally in a water and fire-proof safe. Previous versions of back-up copies should be converted to enable reading when technology changes.

## 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. The level of security built into 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 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. Original data received on paper should stay in a paper file or be image scanned to password-protected 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 Epidemiology 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 are accessible to casual inspection, and require no special expertise to gain access. 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 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 other 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.

(For disposal of electronic records see 5.8.1 (i))

### 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 5-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

- As a general rule, only data to a specificity needed for the question raised should be released.
- The release of aggregate data, in tabular or equivalent formats, and anonymised data does not usually breach confidentiality.
- 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.

An example of disclosure control guidance is available at [www.statistics.gov.uk/about/data/disclosure/downloads/confidentiality-guidance.pdf](http://www.statistics.gov.uk/about/data/disclosure/downloads/confidentiality-guidance.pdf)

Many of the uses of registry data, especially in research and quality control for e.g. screening, 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 legalise the use and the release of data for preventive medicine, including 'public health purposes and scientific research'. National legislation may in the public interest by law or legal order add further exemptions.

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 including ethical standards 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.

- It is advised have a data transfer agreement signed with the receiving part of the data, specifying the terms for use and publication of the data.

### **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 legislature concerning the transfer and release of medical (clinical) data in the country.

### **6.4 Release of identifiable data for scientific and cancer control 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, including a model transfer agreement (see 6.1) 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. The release should fall within the accepted uses of registry data and the requirements for safeguarding the confidentiality of the data.

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.

The requesting party should also make 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:

- (f) Observe the same principles and obey the same laws as are observed and obeyed 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.
- (h) 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 authorisation to do so has first been obtained from the treating physician. When appropriate, approvals by ethics committees should also be sought.
- (i) Ensure that no publication of the results will enable any individual to be identified.
- (j) Report in writing to the cancer registry director when the data are disposed of, returned or destroyed as agreed.
- (k) Give due acknowledgement to the registry for provision of the data.
- (l) 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**

If the cancer registry holds the full ID of the patients; 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). If 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) this obligation does not apply.

It is recommended that such data are released either through the treating physician or 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. 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.

## **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 should only be done when necessary. When the study design requires that identifiable data be transmitted across registry or national borders this can be done within the European Union and EFTA. Outside these countries, 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

---

- 1 European Network of Cancer Registries. *Guidelines on confidentiality for population-based cancer registration in the European Union*. Lyon, International Agency for Research on Cancer and European Commission, February 2002.
- 2 International Association of Cancer Registries. *Guidelines on confidentiality in the cancer registry. Internal report no. 92/003*. Lyon, IARC, 1992.
- 3 Coleman MP, Muir CS, Ménégoz F. Confidentiality in the cancer registry. *Br J Cancer* 1992; **66**: 1138-49.
- 4 International Association of Cancer Registries. Guidelines on confidentiality for population-based cancer registration, Internal report No. 2004/03. *International Association of Cancer Registries* 2004.  
<http://www.iacr.com.fr/confidentiality2004.pdf>
- 5 Doll R
- 6 Hansson MG. *Need for a wider view of autonomy in epidemiological research*. Uppsala University, 2010. *BMJ*. 2010 May 5;340.
- 7 Council and Parliament. Protection of individuals with regard to the processing of personal data and on the free movement of such data. Directive 95/46/EC; OJ L.281/31:31-50. 24-10-1995.
- 8 Storm HH, Clemmensen IH, Black RJ. *Survey of cancer registries in the European Union. IARC Technical Report No. 28*. Lyon, IARC, 1998.
- 9 Barrett G, Cassell JA, Peacock JL, Coleman MP. National survey of British public's views on use of identifiable medical data by the National Cancer Registry. *Br Med J* 2006; **332**: 1068-72.
- 10 Lowrance WW. *Learning from experience: privacy and the secondary use of data in health research*. London, Nuffield Trust, 2002.
- 11 Lowrance WW. *Privacy and health research. A report to the US Secretary of Health and Human Services*. Washington, DC, DHHS, 1997.
- 12 Lowrance WW. *Access to collections of data and materials for health research. A report to the Medical Research Council and the Wellcome Trust*. London, Medical Research Council, 1 March 2006.
- 13 Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. *For the record: protecting electronic health information*. National Research Council, Washington, DC, 1997.
- 14 Jensen OM, Parkin DM, MacLennan R, Muir CS, Skeet RG (editors). *Cancer registration – principles and methods*. IARC Scientific Publication No. 95. IARC, Lyon, 1991.
- 15 Fritz A, Percy C, Jack A, Shanmugaratnam K, Sobin LH, Parkin DM, Whelan SL, eds. *International Classification of Diseases for Oncology (ICD-O), third edition*. Geneva: World Health Organisation; 2000.
- 16 IEA (International Epidemiology Association) November 2007.  
[http://www.ieaweb.org/index.php?option=com\\_content&view=article&id=15&Itemid=43&showall=1](http://www.ieaweb.org/index.php?option=com_content&view=article&id=15&Itemid=43&showall=1)
- 17 Muir CS, Démaret E, Boyle P. *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, 1985. pp. 13–26.
- 18 Brewster DH, Coebergh JW, Storm HH. *Population-based cancer registries: the invisible key to cancer control*. Scottish Cancer Registry, Information Services, NHS National Services Scotland, Apr. 2005. *Lancet Oncol* pp 193-5.
- 19 Medical Research Council. *Responsibility in the use of personal medical information for research: principles and guide to practice*. *BMJ* 1985; 290:1120–1124.
- 20 Anderson RJ. *Security in clinical information systems*. University of Cambridge (internet publication <http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html>) and BMA; 1995.
- ... Royal College of Physicians Committee on Ethical Issues in Medicine. *Research based on archived information and sample*. *J R Coll Phys Lond* 1999; 33:264–266.



---

## APPENDIX

### **Confidentiality issues regarding population based cancer screening monitoring systems and registries.**

Screening for cancer is a prevention strategy with the aim of early detection of presumptive lethal disease in order to decrease morbidity and mortality of cancer. Screening is an intervention towards a "healthy" population and although the individual person may perceive the benefit it can only be measured in terms of decreased morbidity and mortality in the population. Negative side-effects like false positive outcome, or false reassurance, worry and anxiety related to the testing is an ethical concern hence the WHO guidelines for implementing screening must be adhered to (1)- (<http://www.who.int/cancer/detection/variouscancer/en/index.html>). In addition to these it is only ethical to intervene with screening in a population if the screening is organised and there is access to relevant data at an individual level enabling to ascertain the quality and optimal outcome of the entire screening process.

The European Council recommends population-based screening for cancer of the cervix uteri, breast in women and of for colorectal cancer in women and men offered in organised programmes in agreement with evidence based guidelines (2-4).

A screening registry is the cornerstone of a population based and centrally organised screening programme. The purposes is to have a monitoring system for the quality assurance and audit of the screening programme with access to the target population and the ability to store data on the entire chain at an individual level from invitation to participation and testing, further assessment and treatment. In the absence of population based cancer registries also to evaluate the effect and the long term results and form the basis for research. It should contain relevant data on screened individuals (such as: unique ID, sex, birth date, residence, the date and results of the screening tests and follow-up examinations). The role of a cancer screening registry in the framework of a comprehensive cancer prevention policy is described in Table X. To fulfil its full role, the screening registry should contain all screen test results and not only the positive cases. All screened individuals should be entered irrespective of their age or the type of screening (organised or opportunistic).

**Table X.** Role of a cancer screening monitoring system and registrar:

- 
- Monitoring of the entire screening process
  - Direct service to citizens:
    - invitation of individuals belonging to the target population to attend for a screening: call system (invitation of all individuals of the target age group) or call-recall (invitation of individuals of the target age group who did not have a known recent screening test),
    - fail-safe system to recover screen-positive individuals lacking follow-up,
    - information to GPs and other health professionals with respect to the screening status and history of their patients.
  - Process evaluation:
    - response rate to invitation, screening coverage,
    - distribution of screen test results, positive predictive value of positive screen tests, detection of cancer or high-grade cancer precursors; compliance with recommended follow,
  - Impact evaluation
    - audit of cancer cases
    - comparison of interval cancer rate, cancer rate among non-screened populations
    - effectiveness of cancer screening using a case-control study design (screening and follow-up history of cancer cases versus matched controls without cancer)
- 

A screening registry should be linkable with population files, follow-up registries (colposcopy; colonoscopy; additional imaging, histological biopsies; therapeutic interventions), HPV vaccination registries, the national or regional cancer registry, biobanks (cell or tissue specimen of cervix, colon, breast) and mortality registries. A unique ID is needed allowing these linkages if accepted by the relevant controlling bodies in accordance with the derogations to the data protection Directive 95/46/EC.

The confidentiality principles for cancer registries should be applied for screening registries as well. However, a more comprehensive legislative framework as foreseen in the European Council recommendation may be needed since screening registries comprise not only cancer patients but the whole population of certain target age groups, with the large majority being healthy and not presenting symptoms.

A screening registry must operate in agreement with national privacy legislation, laws regulating biobank practice and patient rights. Informed consent or opt-out are two possible procedures assuring that screening data never are registered outside control of the individual concerned. In the former, a priori absence of consent and, in the latter, automatic consent, unless explicit refusal, are assumed. In Belgium cancer screening

data is recognised in the privacy protection law as an example where such derogation is accepted (5) alongside the obligatory registration of all cytopathological results in the framework of early detection of cancer (6).

In Sweden, access to individual data on the entire population is approved for the reason of equality and quality assurance of all phases of a screening programme in order to ensure the population of equal access to the screening programme and equal access to optimal assessment, treatment and follow-up. When data in a screening register is used for such purposes, they are regarded as patient records and the register as a *care register*. When a same register is used for other purposes e.g., research or evaluation at a group level, data are regarded as quality data and the register as a *quality register* and access would not be allowed without an approval from an Ethical Board. M. Arbyn (Unit of Cancer Epidemiology, Scientific Institute of Public Health, Brussels, Belgium

S. Törnberg (Stockholm, Sweden)

## REFERENCES

1. WHO, Screening for cancers; <http://www.who.int/cancer/detection/variouscancer/en/index.html> July 12 2011
2. Arbyn M, Anttila A, Jordan J, Ronco G, Schenck U, Segnan N et al. European Guidelines for Quality Assurance in Cervical Cancer Screening. Second Edition - Summary Document. Ann Oncol 2010; 21: 448-58.
3. Perry N, Broeders M, de Wolf C, Tornberg S, Holland R, von Karsa L. European guidelines for quality assurance in breast cancer screening and diagnosis. Fourth edition--summary document. Ann Oncol 2008; 19: 614-22.
4. Council of the European Union. Council Recommendation of 2 December 2003 on Cancer Screening. Off J Eur Union 2003; 878: 34-8.
5. Segnan, von Karsa .... European Guidelines for Quality Assurance in Colorectal Cancer Screening. First Edition 2010.
6. Arbyn M, Wallyn S, Van Oyen H, Nys H, Dhont J, Seutin B. The new privacy law in Belgium: a legal basis for organised cancer screening. Eur J Health Law 1999; 6: 401-7.
7. Federal Public Service for Public Health (Federale Overheidsdienst Volksgezondheid, Veiligheid van de Voedselketen en Leefmilieu Service publique fédéral Santé publique Sécurité de la Chaîne alimentaire et Environnement. Extension of the Royal Decree on Cancer Registration with respect of cytopathology registration of acts related to early detection of cancer. Belgisch Staatsblad/Moniteur belge , 34360-34361. 2-6-2010.
8. Törnberg S, Screening for early detection of cancer: Ethical aspects. Acta Onc 1999;38:77-81.