Chapter 15. Cancer registration: legal aspects and confidentiality

C.S. Muir and E. Démaret

International Agency for Research on Cancer,
150 cours Albert Thomas, 69372 Lyon Cédex 08, France

Introduction

That an individual is entitled to medical care seems obvious. Health care involves not only diagnosis and treatment of disease but also prevention, control and measurement (registration). With the public's growing awareness of the confidentiality issue, and concern over individual privacy, including the linking of medical and non-medical files, safeguarding the confidentiality of medical and other personal information has become increasingly important. In consequence, legislation in support of an individual's right to privacy is being enacted in many countries. The measures taken by some governments in this direction have, however, frequently resulted in legislation and data protection regulations that impose confidentiality measures which may not be consistent with, or indeed militate against, the optimal use of cancer registry data.

Data protection sometimes do not protect the data, but encourage their destruction, when their preservation—and protection, *sensu stricto*—would be of much epidemiological value. Many files which have avoided destruction (deliberately or accidentally) have proved to be of great importance in subsequent studies, whilst the abuse of such files remains to be demonstrated. Data in cancer registries never lose their value, and data collected as long as 40 or 50 years ago are still used frequently.

The legal basis of cancer registration

Cancer registration may be based on voluntary or compulsory notification of patients. Compulsion may result from legislation or from an administrative order issued by a statutory body, such as the Ministry of Health, or a provincial health authority. In some areas reporting may be both voluntary and compulsory, depending on the source of notification. For example, in one registration area pathologists may report voluntarily, while the Vital Statistics Office is compelled to do so; in another, pathologists may be required to report cancer by law, while treating physicians would do so on their own initiative. Unless cancer is a legally reportable disease, the cancer registry is in effect operating on a voluntary basis. In some countries, this could imply the patient's explicit consent to the entry of information in an identifiable form into

the registry. It should be stressed that voluntary reporting does not necessarily mean less complete reporting. In most countries reporting is still voluntary, and in several such areas cancer registration is of equal or higher quality than in areas with compulsory reporting.

The expanded collection and use of information about individual members of society which has been made possible by the technological developments in recent decades has led to heightened public concern about privacy and confidentiality issues. In this context, the legal aspects of cancer registration have become increasingly important. However, administrative or statutory provisions may both help and hinder registration. To make cancer a reportable disease by law may increase reporting and clarify the position of the person or institution reporting. On the other hand, privacy protection laws may make registration of identifiable data impossible or allow cancer patients to refuse registration. The Hamburg Cancer Registry, for example, saw the number of annual new cases reported decrease from 10 000 before 1980 to 2 in 1980–1981, owing to the apprehension of physicians about possible consequences of reporting to the registry. This arose from a modification of the rules for transmission of confidential data between the cancer registry and the Ministry of Health, the major notification source—a legal basis for such cooperation did not exist. A new law came into effect in 1985, allowing physicians to report cases to the cancer registry, but subject to patient consent.

Cancer registries and the users of cancer registry data have a strong mutual interest in ensuring that cancer registries will continue to collect high-quality data and that data will be used as effectively as possible, consistent with preservation of the anonymity of data subjects.

The aims of confidentiality

As noted in Chapter 3, the aim of any cancer registry is to make aggregate and individual data accessible for medical, research and statistical purposes. To be of value, data recorded must be accurate, reliable and as complete as possible. Both the procedures of registration and the maximal use of the data make it essential that individuals can be identified. Accuracy and completeness can be achieved only if the public and the treating physician are confident that the data required are necessary for the aims and objectives of the registry and that the data will be safeguarded. Safeguarding the data in the cancer registry implies not only that they are sufficiently secured against unauthorized access, but also that they are not used for purposes other than those for which they were collected.

The aims of confidentiality measures in cancer registration are thus to ensure (*a*) the preservation of anonymity for individuals reported to the registry and if necessary also for those making such notifications; (*b*) that cancer registry data are of the best quality possible, and (*c*) that the best possible usage of cancer registry data is made for the benefit of the cancer patient, for cancer control and for medical research.

Preservation of confidentiality

In order to preserve the anonymity of the data reported to them, cancer registries are advised to establish a code of conduct. Confidentiality applies not only to data on

cancer patients, but also to those on other individuals, e.g., members of industrial or other cohorts, held by or provided to the cancer registry, and does not depend on whether the information refers to deceased or living persons. In some registries, the anonymity of the notifying physician or hospital department must also be maintained.

The director of the registry is responsible for maintaining confidentiality and this responsibility should be defined in appropriate legislation or by administrative order. However, the preservation of confidentiality is the concern of all staff within the registry and, at the time of employment, it is recommended that staff sign a special declaration, to the effect that no information on data in the cancer registry will be disclosed. It should be made clear that breach of this undertaking will result in disciplinary action. It is important to stress that this oath of secrecy remains operational even after employment ceases. Reminders concerning the need to preserve confidentiality may be posted within the registry, and it is recommended that cancer registries formally review confidentiality measures at appropriate intervals.

Practical aspects of confidentiality in cancer registration

Information reaches the registry by well-defined paths (see Chapter 5), it is normally treated according to a set of operational rules (see Chapters 6 and 7) and a series of reports or other outputs prepared (see Chapter 10). Several outputs are for internal use only. It is useful to prepare a flowchart of registry procedures and determine where measures to ensure confidentiality need to be applied.

Items which may require specific consideration and some of the measures which may be taken are indicated below.

Collection of notifications

Notifications of cancer patients may derive from many sources such as the treating physician, hospital records room, hospital discharge office, pathology, cytology, haematology and biochemistry laboratories, radiologists, coroners and vital statistics offices (death certificates). These reports generally contain the name of the patient, as well as other identifying information, and it is essential that their contents are not disclosed to parties other than the source and the registry. If registry staff collect source information, they are responsible for the preservation of confidentiality, not only with respect to information on cancer, but to anything of a confidential nature they might happen to see or hear at the source. Consideration should be given to the provision of a lockable attaché case for the transport of data collected by registry staff at source.

Transmission of information from source to registry or from registry to source

Information may be transmitted by mail, tape, diskette, computer terminal or telephone.

Mail

Among the possible security measures which may be considered are (*a*) use of registered mail; (*b*) sending of lists of names and other information separately; (*c*) use of plain envelopes; and (*d*) use of double envelopes, the exterior giving a general address, the interior to be marked 'to be opened by X only'.

Magnetic media

When information is sent on magnetic tape, diskette or other comparable media, precautions should be taken to ensure (*a*) that these do not go astray; (*b*) that they are not easily read by third parties; and (*c*) that they do not leave the registry premises without authority.

Among the precautions that may be taken are: the encrypting of names, which may be done to various levels of complexity, and the preparation of separate tapes or diskettes for names and addresses and tumour-related data, incorporating a link number and giving maximum security to the name tape. It is advisable to keep records of all magnetic tapes, diskettes, or other data media leaving and received by the registry.

Computer

Information may be transmitted via computer, and a registry may send its information for storage on an external computer. Among the precautions that should be taken are the use of user identification and passwords (which preferably should not appear on the VDU when entered), the recording of time of utilization of those authorized entry and the checking of such information against a log-book to be completed by the user. Passwords should change at intervals. Consideration should be given to the encrypting of names during transmission. As information systems evolve, it is likely that an increasing amount of data will be sent to cancer registries on a public or dedicated telephone line.

Telephone

Sometimes the telephone may be used to obtain information from the source, or from the registry, in particular to complete missing information. It must be recognized that the telephone, although convenient, may give rise to breach of confidentiality. No confidential information should be given on the telephone unless the caller is an authorized recipient and, further, has given proof of identity.

Access to and storage of data

Registry

Unauthorized access to the cancer registry must be prevented. It is recommended that a written list of persons currently having access to the registry be established. The necessary control, locking and alarm systems should also be installed.

Computer

The majority of the information in the cancer registry is stored in the computer, which is not readily accessible to the uninitiated. Access to the data in the computer is normally protected by the use of passwords. A further security measure is to keep the name file separated from the rest of the information, with a special key or password to gain access to the name file. Encrypting of names may also be considered. The director of the registry should maintain a list of registry staff members indicating the type and level of data to which each of them has access. At the end of the working day external storage media, such as tapes and diskettes should be kept in locked fireproof safes.

Paper files

Most registries still hold a considerable amount of data on paper which is easily read. This material could include, for example, notification forms, case records for extraction, copies of pathology reports, copies of death certificates etc. It is not practicable to keep names and other information separate for such material. Consideration must thus be given to keeping this information as secure as possible. Among the measures that might be considered are (*a*) defining who has access to the registry premises (see above); (*b*) defining which members of personnel have access to the rooms where this material is kept; (*c*) providing lockable cabinets into which the material would be put at the end of the day's work; and (*d*) ensuring that unauthorized staff (e.g., cleaning personnel) are unable to scrutinize records—this includes carbon copies and other waste paper.

Disposal of dead files. Many registries keep paper files for, say, two years after a registered patient is known to have died. Such files are then microfilmed, the film being stored indefinitely, and the originals destroyed. Such destruction should normally involve shredding or burning.

Cessation of registry activity

Each cancer registry should have a policy for the action to be taken in case the registry ceases its activities. It is recommended that on cessation all records in the registry be microfilmed and stored for a minimum of 35 years, by an appropriate body, which should engage to observe the same confidentiality rules as the cancer registry when in operation.

Use and release of data

If a registry is to meet its mandate, its data must be released for use. Some of the purposes for which data are released may, however, pose problems of confidentiality.

Confidential data should be provided by the cancer registry only on written request. The request should include (*a*) the exact purpose for which data are needed; (*b*) the information required; (*c*) the name of the persons who will be responsible for keeping the confidential information; and (*d*) the time period for which the data are needed.

When confidential data are requested it has to be confirmed that (*a*) those receiving the data are bound by the principles of confidentiality observed by the personnel of the cancer registry; (*b*) the recipient conforms to the restrictions on the use of the data, specifically that they are not used for purposes other than those agreed upon at the time of provision and that the data are not communicated to fourth parties; (*c*) contact with patients, or members of their family, whose names have been provided in confidence by the cancer registry, is established only *after* obtaining the authorization of the physician in charge of treatment; and (*d*) data which are no longer needed for the designated purpose will be returned or destroyed.

Diagnostic and treatment purposes

Data may be provided to physicians for diagnostic or treatment purposes. As diagnosis and treatment are increasingly a team effort, which means that confidentiality is shared, rules for data release have to take this into account.

Statistical and research purposes

Use and release of data for statistical and research purposes aim at advancing knowledge for the benefit of the individual, at improving health and health services and at assisting in health administration and planning.

Aggregate data. One of the most important contributions the cancer registry can make is to provide current data on the incidence of cancer by age, sex, place of birth, occupation etc. Differences in histological type or urban/rural differences can be examined, as well as time-trends. Such tabulations rarely give rise to problems of confidentiality. Although it is potentially possible to identify individuals in a table, when there are very small numbers in a cell, the risk that this would actually be done is extremely small. Tables should, however, be devised so as to minimize the risk, and the level of detail to appear in routine registry reports should be considered (e.g., number in cells, identification of source, survival by source, rate by area etc.).

Individual data. Case–control or cohort studies help to identify the causes of cancer. Cancer registries are important contributors to such investigations and the cancer registry may, for example, be asked to supply names of people with a given cancer so that they can be included in a case-control study. Names should not be divulged unless the attending physicians have given their consent for each patient, or alternatively names may be disclosed to bona fide researchers with a proviso that patients or any other person must not be approached without the prior permission of the attending physician or hospital department. For the majority of investigations, the reporting of anonymous or group data are sufficient. It should be emphasized that published epidemiological investigations never divulge the identity of the persons in the study.

International release

Data shall not normally be forwarded to other countries in a form which permits the individual to be identified. For the purposes of further verification in the country of origin, each study subject may be allocated a consecutive number or other designation

by which the individual can, when necessary, be traced in the cancer registry of origin by the registry staff. When the circumstances of a study require, and national legislation permits, that individual data cross national borders, e.g. for a study of migrants, such data should be subject to the rules of confidentiality of the providing nation.

Administrative purposes

Confidential information must not be provided for life insurance, sick funds, pension schemes, or other such administrative purposes, nor to a physician examining an individual for such purposes.

Dissemination of data in periodic reports, to official bodies, press and general public

Data disseminated through annual or other reports, while being aggregate and, in consequence, anonymous, should be presented so as to make the potential identification of an individual impossible.

Cancer registries are frequently approached by the press for information on a variety of topics. It is recommended that a specially designated person be appointed within the cancer registry to handle such enquiries.

Cancer registries are not infrequently asked to demonstrate the system. It is recommended that, when such demonstrations are given, the data used be fictitious and labelled as 'Demonstration' so that onlookers are aware of this. For such occasions it may be useful to use a special password.

Record linkage

Linkage of records for individuals is essential if cancer is to be measured accurately (Chapter 8), the causes of cancer ascertained at minimum expense and the effect of control measures assessed. Linkage requires that records carry information on identity.

Linkage with external files may be done in order to (*a*) follow up for survival; (*b*) follow up for treatment outcome; and (*c*) carry out epidemiological studies. The confidential nature of the data must be respected, whether matching is done within the registry or outside. The same applies when, on matching, a case unknown to the registry is found, on which the registry needs more information from the source.

If matching has to be done outside the registry, e.g., in a vital statistics office, or on a computer belonging to a third party, the registry must ensure that confidentiality of the registry records will be preserved and that the body receiving the registry data will observe a no lesser degree of confidentiality. Similarly, if matching is done within the registry with outside records, the same confidentiality rules should be applied.

When, following a match of registry files and death certificates, a death certificate only (DCO) case is identified and the registry seeks further information about that case, the request for such information shall be made to the certifying physician. If national policy so dictates, this approach may need to be made through the vital statistics office.

If, on matching with other files, a registry suspects the existence of a hitherto unregistered case, the registry shall approach the organization responsible for that data file to obtain further information, if that organization itself is bound by confidentiality rules.

Unauthorized access to the computer system

There have been examples of persons who have succeeded in breaking into computer systems, either to steal information or more often just to show that this is possible. The authors are not aware that this has ever happened in a cancer registry. While it is unlikely that registries would be able to protect their systems completely, the level of security built in should be such as to foil casual attempts to gain access. An isolated data processing facility dedicated to the cancer registry increases the security.

Summary

Some of the security measures which may be taken are:

(*a*) limited and well-defined access to the registry;
(*b*) limited and well-defined access to the computer room;
(*c*) limited and well-defined access to the computers, with passwords giving access to information;
(*d*) passwords and user keys which do not appear on the VDU;
(*e*) recording of computer time used by each authorized person;
(*f*) separation of the name file from other files, with encoding or scrambling of names;
(*g*) provision of lockable attaché cases to staff members who transport confidential information;
(*h*) provision of a means of identification of registry staff;
(*i*) particular attention paid to preserving the confidentiality of data when collecting, transmitting (whether by mail, tape, diskette, computer or telephone), storing, releasing and matching;
(*j*) creation of control measures for any output permitting identification of individuals;
(*k*) restriction of the right to match registry files with external files.

Above all the director of the registry must imbue the staff with the need to maintain a high level of security and hence preserve confidentiality.

Conclusion

In several countries the public has become increasingly aware of the confidentiality issue, in particular following the wider use of computers and the storage of data in them: concern is largely linked to a fear of 'names in the computer'. Yet locked up in a computer, accessible only to those with special knowledge and the right of access, names are much safer there than on bits of paper. Computer encrypting techniques are now such that they are for practical purposes unbreakable.

The matching of names of cancer patients with other non-medical files is of

legitimate public concern. The Nordic countries have data protection boards which approve such matching on a study-by-study basis. In England and Wales the approval of the Ethical Committee of the British Medical Association is needed. Such open authorization, given after the investigator has explained his or her aims, is likely to control abuse and improve the quality of studies.

Cancer registries have long been regarded as contributing substantially to cancer patient and community care, and in so doing have maintained their own codes of confidentiality. Many registries, however, do not have a written code. It is recommended that cancer registries draft their own rules and regulations, based on the general principles outlined here and adapted to the registry's local situation[1].

Absolute secrecy, with the only persons knowing about the cancer being the patient and the attending physician, in effect means that the individual cancer patient is prevented from benefiting from the experience of others with cancer and from contributing to the pool of knowledge about the disease. Such secrecy makes it easier for industrial and other risks to remain uncovered or deliberately concealed, and it prevents the collectivity from assessing the value received from funds invested in treatment, screening and prevention programmes. The authors are not aware that any cancer registry has breached confidentiality. Those who continue to oppose ethical cancer registries bear a heavy responsibility.

[1] A document entitled *Preservation of Confidentiality in the Cancer Registry* has been prepared by the International Agency for Research on Cancer, and is available on request.