8
Confidentiality of medical records

The primary goal of a population-based cancer registry is to collect data which are as complete,accurate and reliable as possible. To be able to achieve this, the registry needs the cooperation of health professionals and the general public, who would like to be assured that the information being gathered is necessary to meet the objectives of the registry and will be safeguarded against unauthorized access and misuse.

With the public's growing concern for individual privacy and medical confidentiality, safe keeping of medical information has become increasingly important. Unless measures are taken by the registry to ensure the preservation of medical confidentiality, problems will be encountered in cancer registration, especially by population-based registries. The aim of establishing these measures is to ensure that information on the cases reported to the registry is not divulged to unauthorized individuals or organizations

Medical confidentiality is not limited to medical information on cancer patients held by physicians and medical institutions. It also includes data on other individuals, such as members of cohorts on whom data are stored in the registry, as well as information gathered from death certificates.

The preservation of confidentiality concerns all members of the registry staff. It is recommended that, at the time of employment, every member should sign a special undertaking to preserve the anonymity of the registry data and not to divulge any information, even after employment ceases. Disciplinary action should be considered if the rules are broken.

Each cancer registry should have its own set of rules and regulations of confidentiality, applicable to its own setting. A copy of the rules should be given to all staff on arrival, and also be posted within the registry premises as a constant reminder.

Practical aspects of confidentiality in cancer registration

Measures to ensure confidentiality can be implemented in the different operations of the registry, i.e. data collection, data transmission, in-put procedures, storage, and preparation of reports:

1. Data collection

Information on cancer patients may be gathered actively, or notifications may be sent to the registry by the different data sources in the hospital(s) and by the vital statistics bureau. The contents of these reports should not be disclosed to other parties than the data source and the registry. If the data are collected actively, it is the responsibility of the registry staff to preserve the confidentiality of information on cancer cases or anything of a personal or confidential nature seen or heard at the source. It is highly recommended that the data collected be kept under lock and key, preferably in a lockable case, until they reach the registry. The data should not be left in a place where an unauthorized person might have access, e.g., in a car.

2. Data transmission

Transmission of information may be accomplished by several methods. Different security measures may be considered for each mode of transmission:

(a) Mail:

When sending information through the mail staff may:

(i) use registered mail;

(ii) send the medical information separately from the list of names, with a 'key', so they can be put back together;

(iii) use double envelopes: the exterior one gives a general address and the interior envelope is marked "to be opened by X only".

Confidential data should never be sent by fax.

(b) Magnetic media:

When information is sent on magnetic tape or diskette, it is important to take measures to ensure that these will not go astray, will not be easily read by other parties, and do not leave the registry premises without authority.

The following precautions may be taken:

(i) encrypting of names at various levels of complexity so that they cannot be read easily by other parties;

(ii) preparation of separate tapes, or diskettes, one with the names and addresses and another with the tumour-related data, incorporating a common link number.

(iii) keeping a record of all magnetic tapes, diskettes or other magnetic media sent and received by the registry.

(c) Telecommunications:

Particular care should be taken when transmitting data by internet. If it is absolutely necessary to use names these must be encrypted.

(d) Computer:

If a registry stores its information on a computer, user identification and passwords (which preferably should not appear on the VDU screen when entered) should be used. Passwords should be changed regularly. Identifying information must not be included when data are transferred from the computer.

(e) Telephone:

Confidential information should not be given over the telephone, nor should enquiries from collaborators concerning confidential data be answered over the phone (e.g., danger of crossed wires). If the telephone is used by staff to complete missing information in the registry, this may be given only if the caller is an authorized recipient and can give proof of identity. The registry staff should not give confidential information over the telephone as this would constitute a breach of confidentiality.

3. Access to and storage of data

(a) Registry:

The registry director should establish a written list of persons who currently have access to the registry, indicating the levels of access authorized. All registry records should be stored in a room which can be locked and access to which is limited only to authorized persons.

(b) Computer:

In a computerized registry, part of the information is kept in the computer, and access to the data is protected by the use of a password. Other security measures to be considered are to:

(i) use a name file which is separate from the other information;

(ii) encrypt the names at various levels of complexity;

(iii) prepare a list of staff with access to the data including the level of access for the registry director;

(iv) put electronic data processing material, e.g. back-up and other tapes, in a locked, fire-proof safe at the end of the working day.

(c) Paper files:

Since these files could be read easily by an outsider, additional security measures to ensure their confidentiality should be considered:

(i) defining who should have access to the registry premises;

(ii) defining who should have access to the room where the records are stored;

(iii) providing a lockable cabinet to keep all records, including back-up copies, at the end of the working day;

(iv) confidential waste paper should be shredded in order to prevent unauthorized staff (e.g., cleaning personnel) from scrutinizing the records.

(d) Dead files:

Paper files containing the names of persons who have died from cancer may be kept in the registry for about two years and then put on microfilms (if resources allow) which

are stored indefinitely. The original files are destroyed either by shredding or burning.

(e) Cessation of activity:

It is recommended that if and when the registry ceases its activities, all records in the registry should be microfilmed and kept for a minimum of 35 years by an appropriate body, which should observe the same rules of confidentiality as the cancer registry when it was still in operation.

4. Use and release of data

Confidential data may be provided by the registry only upon written request, which should include the exact purpose for which the data will be used, the information required, the name(s) of the person(s) responsible for keeping the confidential information, and the time period for which the data are needed.

Before any confidential data are released, the registry should make sure that those receiving the data:

(i) are bound by the same rules of confidentiality observed by the registry staff;

(ii) will use the data only for the purpose agreed upon at the time of provision, and will not make them accessible to other parties;

(iii) will return or destroy the data when they are no longer needed for the said purpose; and

(iv) will not contact a patient or members of his/her family unless authorization is granted by the attending physician.

No information should be provided to insurance companies, medical funds, pension schemes, employers, the police, the authorities, etc., nor to a physician having to examine an individual for such purposes.

(a) Aggregate data:

One of the most important activities of the registry is the preparation of incidence data by age, sex, site, and urban/rural distribution, as well as time trends. Usually this does not pose any problems in confidentiality, except when there are very small numbers in a cell. Thus, in the preparation of reports, care should be taken not to go into very minute details sufficient to identify individuals in any cell of the tabulation.

(b) Individual data:

Cancer registries contribute to investigations on the causes of cancer and the registry may frequently be asked to provide the names of patients with a given cancer so that they can be included in, for example, a case-control study. Patients' names must not be disclosed unless the attending physician of each patient gives his/her consent. Names may be disclosed to bonafide researchers with the agreement that the patient or members of the patient's family must not be approached unless the attending physician or the hospital department permits them to do so. The published results of any study must not identify any individual, or include any detailed information which permits such identification.

(c) International release:

Data sent abroad should be in a form which does not permit individual identification, or a code number (e.g., patient registry number) should be used, which would not permit identification of the individual in the cancer registry of origin. In a study on migrants, where individual data have to be sent to other countries, these data should be subject to the rules of confidentiality of the providing nation.

(d) Record linkages:

Registry files may be linked with external files for research purposes. Security measures must be taken to protect all identifying information.

If on matching with other files a registry suspects the existence of an unregistered case, the registry should approach the organization responsible for the data file to obtain further information.

(e) Dissemination of data in periodic reports, to official bodies, the press and the general public:

Annual or periodic reports should be presented in tabular form or in graphs or histograms, making individual identification impossible.

Someone in the registry, usually the director, should be specifically assigned to answer enquiries from the press on various topics regarding the registry.

Exercises:

QUESTIONS: True or false?

1. Confidentiality measures in the registry ensure the preservation of the anonymity of individuals reported to the registry.
2. Medical confidentiality is limited to medical information on cancer patients held by physicians or hospitals.
3. The maintenance of strict medical confidentiality in the registry is the responsibility of the registry director.
4. Preservation of confidentiality in the registry is the concern of all the members of the staff.
5. Every registry worker should sign a special declaration or "oath of secrecy" to the effect that he/she will preserve the anonymity of the data in the registry, and this is operational even after employment ceases.
6. Data gathered actively from data sources should be safeguarded in transit, e.g., in a lockable attaché case until they reach the registry.
7. Release of registry information to a physician examining a patient for health insurance purposes constitutes breach of confidentiality.
8. Release of information via the telephone should be avoided as this can give rise to breach of confidentiality.
9. As a measure of confidentiality in the registry, there should be limited and well-defined access to the registry.
10. Confidential data should be released by the registry only on written request, after having confirmed that the recipient of the information is bound by the same principles of confidentiality as the registry staff, and that the use of the data is restricted only to those purposes which were agreed upon at the time of provision.
11. When transmitting information on magnetic tapes or diskettes, it is recommended that separate tapes or disks be used for name and address and for the tumour-related information, observing maximum security measures on the tape/disk containing the names.
12. The right to match the registry files with other external files should be limited.

ANSWERS:

1. TRUE
2. FALSE
3. TRUE
4. TRUE
5. TRUE
6. TRUE
7. TRUE
8. TRUE
9. TRUE
10. TRUE
11. TRUE
12. TRUE