WMA DECLARATION ON ETHICAL CONSIDERATIONS REGARDING HEALTH DATABASES

Adopted by the 53rd WMA General Assembly, Washington, DC, USA, October 2002

1. The right to privacy entitles people to exercise control over the use and disclosure of information about them as individuals. The privacy of a patient's personal health information is secured by the physician's duty of confidentiality.

2. Confidentiality is at the heart of medical practice and is essential for maintaining trust and integrity in the patient-physician relationship. Knowing that their privacy will be respected gives patients the freedom to share sensitive personal information with their physician.

3. These principles have been incorporated in WMA statements since the WMA was founded in 1947, in particular by:

    1. The Declaration of Lisbon, that states: "The patient's dignity and right to privacy shall be respected at all times in medical care and teaching";

    2. The Declaration of Geneva, that requires physicians to "preserve absolute confidentiality on all he knows about his patient even after the patient has died";

    3. The Declaration of Helsinki, that states:

        "It is the duty of the physician in medical research to protect the life, health, privacy, and dignity of the human subject"

        "Every precaution should be taken to respect the privacy of the [research] subject, the confidentiality of the patient's information and to minimize the impact of the study on the subject's physical and mental integrity and on the personality of the subject"

        "In any research on human beings, each potential subject must be adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and poten-tial risks of the study and the discomfort it may entail. The subject should be in-formed of the right to abstain from participation in the study or to withdraw con-sent to participate at any time without reprisal. After ensuring that the subject has understood the information, the physician should then obtain the subject's freely-given informed consent, preferably in writing"

1. The primary purpose of collecting personal health information is the provision of care to the patient. Increasingly, this information is held in databases. The database might hold the patient's health record or specific information from it, for example in the case of disease registries.

2. Progress in medicine and in health care is contingent upon the conduct of quality assurance and risk management activities and health and medical research, including retrospective epidemiological studies, which use information concerning the health of individuals, communities and societies. Databases are valuable sources of information for these secondary uses of health information.

3. Care must be taken to ensure that secondary uses of information do not inhibit patients from confiding information for their own health care needs, exploit their vulner-ability or inappropriately borrow on the trust that patients invest in their physicians.

4. For the purpose of this statement, the following definitions are used:

    1. 'Personal health information' is all information recorded with regard to the physical or mental health of an identifiable individual;

    2. A 'database' is a system to collect, describe, save, recover and/or use personal health information from more than one individual whether by manual or electronic means. This definition does not include information in the clinical record of any individual patient;

    3. 'De-identified data' are data in which the link between the patient and the information has been broken and cannot be recovered;

    4. 'Consent' is a person's voluntarily given permission for an action, based on a sound understanding of what the action involves and its likely consequences. In some jurisdictions, the law allows substituted consent to be given on behalf of minors, on behalf of adults who do not have the capacity to consent for themselves, or on behalf of deceased persons.

PRINCIPLES

1. These principles apply to all new and existing health databases, including those run or managed by commercial organisations.

Access to information by patients

2. Patients have the right to know what information physicians hold about them, including information held on health databases. In many jurisdictions, they have a right to a copy of their health records.

3. Patients should have the right to decide that their personal health information in a database (as defined in 7.2) be deleted.

4. In rare, limited circumstances, information may be withhold from a patient if it is likely that disclosure cause serious harm to the patient or another person. Physicians must be able to justify any decision to withhold information from a patient.

Confidentiality

5. All physicians are individually responsible and accountable for the confidentiality of the personal health information they hold. Physicians must also be satisfied that there are appropriate arrangements for the security of personal health information when it is stored, sent or received, including electronically.

6. In addition, medically qualified person(s) should be appointed to act as guardian of a health database, to have responsibility for monitoring and ensuring compliance with the principles of confidentiality and security.

7. Safeguards must be in place to ensure that there is no inappropriate or unauthorised use of or access to personal health information in databases, and to ensure the authen-ticity of the data. When data is transmitted, there must be arrangements in place to en-sure that the transmission is secure.

8. Audit systems must keep a record of who has accessed personal health information and when. Patients should be able to review the audit record for their own information.

Patients' consent

9. Patients should be informed if their health information is to be stored on a database and of the purposes for which their information may be used.

10. Patients' consent is needed if the inclusion of their information on a database involves disclosure to a third party or would permit access by people other than those involved in the patients' care, unless there are exceptional circumstances as described in para-graph 11.

11. Under certain conditions, personal health information may be included on a database without consent, for example where this conforms with applicable national law that conforms to the requirements of this statement, or where ethical approval has been given by a specially appointed ethical review committee. In these exceptional cases, patients should be informed about the potential uses of their information, even if they have no right to object.

12. If patients object to their information being passed to others, their objections must be respected unless exceptional circumstances apply, for example where this is required by applicable national law that conforms to the requirements of this statement or nec-essary to prevent a risk of death or serious harm.

13. Authorization from the guardian of the health database is needed before information held on databases may be accessed by third parties. Procedures for granting authori-zation must comply with recognised codes of confidentiality.

14. Approval from a specially appointed ethical review committee must be obtained for all research using patient data, including for new research not envisaged at the time the data were collected. An important consideration for the committee in such cases will be whether patients should be contacted to obtain consent, or whether it is accept-able to use the information for the new purpose without returning to the patient for further consent. The committee's decisions must be in accordance with applicable na-tional law and conform to the requirements of this statement.

15. Data accessed must be used only for the purposes for which authorization has been given.

16. People who collect, use, disclose or access health information must be subject to an enforceable duty to keep the information secure.

De-identified data

17. Wherever possible, data for secondary purposes should be de-identified. If this is not possible, however, the use of data where the patient's identity is protected by an alias or code should be used in preference to readily identifiable data.

18. The use of de-identified data does not usually raise issues of confidentiality. Data about people as individuals, in which they retain a legitimate interest, for example a case history or photograph, require protection.

Data integrity

19. Physicians are responsible for ensuring, as far as practicable, that the information they provide to, and hold on, databases is accurate and up-to-date.

20. Patients who have seen their information and believe there are inaccuracies in it have the right to suggest amendments and to have their comments appended to the informa-tion.

Documentation

21. There must be documentation to explain: what information is held and why; what consent has been obtained from the patients; who may access the data; why, how and when the data may be linked to other information; and the circumstances in which data may be made available to third parties.

22. Information to patients about a specific database should cover: consent to the storage and use of data; rights of access to the data; and rights to have inaccurate data amended.

Management

23. Procedures for addressing enquiries and complaints must be in place.

24. The person or persons who are accountable for policies, procedures, and to whom complaints or enquiries can be made must be identified.

Policies

25. National medical associations should cooperate with the relevant health authorities, ethical authorities and personal data authorities, at national and other appropriate ad-ministrative levels, to formulate health information policies based on the principles in this document.