CODE OF PRACTICE ON DATA CONFIDENTIALITY AND THE USE OF DATA FOR MEDICAL RESEARCH

A Introduction

Access to information regarding patients is often required for biomedical and health services research. The original purpose for collecting patient information is to direct patient care and access to this information for research purposes is a secondary consideration.

While clinicians and trained nurses have a general duty under their professional codes of ethics to respect the confidentiality of information encountered in the course of their work, other research staff are not formally bound in this way. All types of staff need to be aware of the special obligations contingent upon the use, for medical research, of name-identified data that were originally collected for some other purpose. Therefore, the information available to research staff should, either exclude the unique personal identification data or, at least, the identifying information is not juxtaposed with confidential information unless the personal information is unintelligible.

Where personal data on individuals who can be identified are held and processed on computer, these data will be subject to the provisions of the Personal Data (Privacy) Ordinance. Applicants are recommended to consult this document. It is the grant holder's personal responsibility to ensure that any conditions relating to data protection in Hong Kong are observed.

These guidelines are based on the Organisation for Economic Co-operation and Development (OECD) Guidelines for Data Protection.

B Voluntary Guidelines on Data Confidentiality

The voluntary guidelines have been based on an international standard for data protection, the OECD Guidelines for Data Protection. As a major international trading centre, Hong Kong has to ensure that its Data Protection Laws are compatible with those of other countries to enable cross-border transfer of information. Failure to comply with an international data protection standard could result in other countries refusing to release information to Hong Kong. As a result the following guidelines were developed:

Collection Limitation Principle

There should be limits to the collection of personal data; such collection should be fair and lawful and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be adequate, relevant and not excessive in relation to the purposes for which they are to be used. Personal data should be accurate and, where

necessary, kept up to date.

Purpose Specification Principle

The purpose for which personal data are collected should be specified not later than at the time of data collection; subsequent use of personal data should be limited to the fulfillment of legitimate purposes already specified or such other as are not incompatible with them.

Use Limitation Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection; subsequent use of personal data should be limited to the fulfillment of legitimate purposes already specified or such other as are not incompatible with them. Personal data should not be disclosed for purposes other than those which have been specified except with the consent of the data subject or by the authority of law.

Security Safeguard Principle

Personal data should be protected by appropriate safeguards against unauthorised access, alteration, disclosure or destruction and against accidental loss or destruction.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data.

Individual Participation Principle

At reasonable intervals and without undue delay and expense, a person should be able to obtain confirmation of whether or not personal data are held of which he is the subject, to have such data communicated to him in an intelligible form, and where appropriate, to have such data corrected or erased.

C Additional Guidelines on Data Confidentiality

In addition to the above, it is considered that additional guidelines may be required in the specific area of health services research. The following are adapted from the "Code of Practice for Use of Name-Identified Data from Statistical Data Collections" used in the Health Department of Western Australia.

1 Requirement for Written Protocols

Any person requesting access to name-identified medical data for research purposes

should prepare a written protocol for the proposed study. This protocol should address ethical issues and be submitted to a properly constituted Ethics Committee. The written approval of the Ethics Committee must be submitted with the application for Health Services Research grants.

2 Written Declaration

All person who are to have access to name-identified data in the course of their employment or studies shall complete a signed declaration binding them to respect the confidentiality of the information contained therein and to follow this code of practice.

3 Paper Records Bearing Name-Identified Information

3.1 Creation and Maintenance

All paper records, including questionnaires and computer printouts, should be created and maintained in such a manner that identifying information is not juxtaposed with confidential medical or personal information, unless that information is unintelligible. For example, identifying data should be physically separated from the main body of the questionnaire immediately after that latter is completed, linkage at a later data being made possible by some sort of code common to both.

3.2 Storage

Paper records containing named data, especially master lists of codes assigned to named individuals, should be kept under lock and key when not in use. Master lists should be stored separately from the paper files to which they refer. Details of coding systems should be stored securely and separately from records containing information in coded form. These provisions should also apply to paper records containing named information that are removed from the institution in which the research is based for any purpose, for example, field work.

3.3 Disposal

Paper records containing named data should be disposed of by shredding or incineration, preferably on the research site, or under supervision of a responsible member of the research team.

4 Records held on Computers

4.1 Creation and Maintenance

All computer records should be created and maintained in such a manner that identifying information is not juxtaposed with confidential medical or personal information unless that information is unintelligible.

4.2 Storage

Master list of codes assigned to named individuals should be sorted in files separate from data files. Access to name-identified records, especially master lists, which are not in use should be prevented by password- and/or read-access protection of computer files. Details of coding systems should be stored separately from records containing information in coded form.

In the use of standalone Personal Computers, identifying information or master lists of codes should be deleted from the hard disk and all diskettes stored under lock and key. The physical security of both the PC and diskettes should be ensured whenever they are not in use.

5 Publication

No publication or public presentation or discussion of results of research based on name-identified data shall include any information that could allow individual subjects to be identified unless the written consent of each such subject has been obtained.

6 Contact with Individual Patients or their Relatives

From time to time a legitimate need arises to contact patients identified through name records, or their relatives, to obtain further information vital to a research study. In all cases, this contact may only be initiated after approval has been sought from the doctor involved in the case at the time that the name-identified record was generated, or the appropriate successor to the doctor, or the medical practitioner responsible for the management of the relevant hospital/ clinic/ institution. This permission, having been obtained, normal rules of consent would apply to the contact with the patient or relative; that is, verbal informed consent only is required if an interview, questionnaire or physical examination (by an appropriately qualified person) is involved, while written informed consent is required if the study required that the patient undergo any technical, invasive, or therapeutic procedures that is not part of their routine medical care.