NSW HEALTH

INFORMATION PRIVACY

CODE OF PRACTICE

Second Edition
December 1998

NSW HEALTH DEPARTMENT

SHP No. (IMCS) 980187
ISBN 0 7347 3007 1

This publication was produced by the Information Management and Clinical Services Branch. Please direct comments to the Manager, Information Development Unit, NSW Health.

For further copies contact:
Better Health Centre
Locked Mail Bag 5003
Gladesville 2111
Ph: (02) 9816 0452
Fax: (02) 9816 0492

This document has been issued as NSW Health Department Circular No:

CPR 99/18

TABLE OF CONTENTS

1 DEFINITIONS AND ACRONYMS

Frequently used terms are defined as follows in the context of this document.

Affiliated health organisation - An organisation or institution listed in Schedule 3 of the *Health Services Act 1997*, formerly Third and Fourth Schedule institutions under the *Public Hospitals Act*.

Area health service - An area health service constituted under the *Health Services Act 1997.*

CEO (Chief Executive Officer) - Under the *Health Services Act,* the Chief Executive Officer of an area health service or a statutory health corporation or the person responsible to the governing body of an affiliated health organisation for management of its recognised establishments and services.

Client/patient - Any person to whom a health care provider owes a duty of care in respect to provision of health care services.

Confidentiality - The restriction of access to personal health information to authorised persons, entities and processes at authorised times and in an authorised manner.

Data - A representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means.

Data administrator - The Director-General delegates overall responsibility for all data owned by the NSW Department of Health to the Data Administrator; ex officio, the Director of Information Management and Clinical Systems Branch takes this responsibility.

Data collection - A store of data captured in an organised way for a specific, defined purpose.

Data custodian - An officer of the Department of Health or an employee of a public health organisation with day-to-day responsibility for a data collection, usually the Director/Manager of the branch or unit where the collection is maintained.

Data sponsor - The person who undertakes the duties of ownership of a data collection owned by the Department.

Data user - A person with authorised access to data.

Department of Health - The NSW Department of Health as established under section 6 of the *Health Administration Act 1982* which performs the functions of supporting the Minister, undertaking system-wide planning, monitoring and guidance, allocating funding, establishing standards, reviewing performance and providing policy advice.

DOCS - Department of Community Services.

External data custodian - A person other than an officer of the Department or a public health organisation, appointed by the Director-General to manage data owned by the Department, who assumes the role of custodian of that data. Examples are the Director of the NSW Cancer Registry and the Heads of academic institutions which have use of such data by agreement.

FOI - Freedom of Information.

Health care provider - A medical, nursing or allied health professional.

Health Information Manager - formerly Medical Record Administrator.

Health record - A documented account, whether in hard copy or electronic form, of a client/patient's health, illness, and treatment during each visit or stay at a public health organisation.

Health (or medical) research - systematic investigation undertaken for the purpose of adding to the body of knowledge pertaining to human health.

Health worker - A health care provider, clerical, administrative, technical or scientific worker, volunteer, student, consultant or other person working in the public health system.

Hospital - Under the *Health Services Act*, an institution at which relief is given to sick or injured people through the provision of care or treatment.

Identifiable information - Any combination of information characteristics concerning an individual which makes it possible to identify that individual.

Information - The meaning assigned to data by means of conventions applied to that data.

Information privacy - The ability of an individual to exercise appropriate control over the extent to which personal information about him/herself is available to others.

Informed consent - A form of consent which has been sought, expressed and recorded and which seeks to ensure that the person to whom the information relates understands the issues set out in section 6.1.

Intranet - A private network that uses the functionality, cost effectiveness and reliability of Internet protocols and can be customised to meet particular needs as regards security requirements, applications etc.

IPC - Information Policy Committee.

IPPs - Information Privacy Principles (see Appendix 1).

Medical practitioner - A person registered to practise medicine under the *Medical Practice Act 1992.*

OECD - Organisation for Economic Co-operation and Development.

Personal health information - Information which concerns a person's health, medical history or past or future medical treatment, and is in a form that enables or could enable the person to be identified.

Potentially identifiable data - Records from which names and addresses have been removed but from which it might still be possible to identify an individual indirectly by using remaining data such as an identity number or some combination of other, not directly identifying data items.

Public health organisation - Under the *Health Services Act*, an area health service or a statutory health corporation, or an affiliated health organisation in respect of its recognised establishments and services.

Public health system - Under the *Health Services Act* consists of all area health services, statutory health corporations and affiliated health organisations in respect of their recognised establishments and services.

Record keeper - The person who has administrative control of a health record, normally the Health Information Manager.

REC - Research Ethics Committee; a committee, constituted in accordance with NHMRC guidelines, which protects the subjects of research and ensures that ethical standards are maintained by reviewing and advising on the ethical acceptability of research proposals.

Security - A tangible set of physical and logical mechanisms which can be used to protect information held in hard copy, computer systems and information and telecommunications infrastructure.

Senior health care provider - The Medical Superintendent, Director of Clinical Services or other supervising senior health care provider, if appropriate.

SHCEC - Statewide Health Confidentiality and Ethics Committee.

Statutory health corporation - A corporation, listed in Schedule 2 of the *Health Services Act 1997*, which provides certain health and health support services other than on an area basis (including The Royal Alexandra Hospital for Children and Corrections Health Service).

Telehealth - The transmission of images, voice and data between two or more health units via telecommunications channels to provide clinical advice, consultation, peer support, education and training services.

Third party - A person involved in the disclosure of personal health information, being neither the individual who is the subject of the information to be disclosed, nor that individual's health care provider at the time disclosure occurs.

Treating health care provider - A medical practitioner or other health care provider who is responsible for care to the client/patient at the time access to personal health information occurs.

Videoconferencing - A two-way audio-visual system for providing health services between remote locations where face-to-face contact is required.

2 INTRODUCTION

This is the second edition of the Information Privacy Code of Practice, which supercedes the first edition, introduced in May 1996. The Code of Practice is the NSW Health Department's major policy document on information privacy. It covers:

- legislation binding on employees of the public health system
- circumstances where disclosure of personal information is authorised
- informed consent for disclosure of information
- general safeguards to be observed when dealing with personal information
- handling health records
- data collections and security.

Relevant policies and procedures have been consolidated with the aim of improving awareness of and access to all policies dealing with information privacy. By bringing relevant policies together in one document with jurisdiction across the whole public health system, consistency of approach is facilitated. References are made where appropriate to other related policies and procedures.

Because the Code needs to be general enough to be broadly applicable to the whole range of services across the health system it is not prescriptive and not all situations or issues which may arise in all environments have been specifically addressed. Depending on circumstances, local procedures and policies may need to be produced to comply with or supplement this Code.

The provisions of the Code are consistent with Australian Standard AS4400 Personal privacy protection in healthcare information systems[1] which includes a requirement that organisations should have a written information policy. The NSW Privacy Committee has provided advice on the development of the Code.

2.1 Purpose

The Code of Practice seeks to:

- ensure personal health information is collected, stored and used in accordance with Information Privacy Principles (see 3.6)
- acknowledge and delineate the responsibility of the NSW public health system to ensure that the privacy of client/patient information is protected
- meet the need of health workers for clear rules on what is acceptable and what is not when dealing with personal health information in order to remove pressure and uncertainty from those who are involved in the day to day administration of such information
- constitute a benchmark which can be used for auditing performance.

Another key objective of the Code is to protect the privacy of clients/patients by ensuring that only demographic information which is necessary to provide care or services is collected. For instance, in the case of a client/patient attending a public health organisation for a routine procedure, collection of name and date of birth would generally be considered justifiable; collection of information which is irrelevant to the planned procedure, such as marital status however should be regarded as unwarranted.

3 SCOPE

3.1 Who is bound by the Code of Practice?

The Code of Practice applies to all employees, contractors and other health workers who, in the course of their work, have access to personal health information in the New South Wales public health system. This includes:

- providers of health services such as doctors, nurses, case managers, visiting providers and allied health staff
- administrators, clerical and service staff
- technical, scientific and laboratory personnel
- auditors
- interpreters
- volunteers
- students
- consultants
- temporary and contract staff
- external custodians of information owned by the Department.

The Code of Practice applies to:

a) Department of Health
b) NSW Ambulance Service
c) the public health system, that being
- area health services, affiliated health organisations and statutory health corporations
- any health service provided by the public health system including nursing homes, hostels and group homes, community health services, drug and alcohol services, allied health programs, dental and early childhood services, multi-purpose services, scientific and laboratory services and health promotion and public health services

d) non-government organisations receiving funding from the Department where compliance is included in the terms of their Funding Agreement
e) private hospitals and day procedure centres treating public patients on a contractual basis (limited to records of public patients)
f) staff of Health Professional Registration Boards (excluding Medical, Dental and Pharmacy Boards).

Where access is granted to information held by the public health system for research or other purposes, the person or organisation granted access should, under the conditions of access, also be required to comply with the terms of this Code.

3.2 What information does it cover?

The Code of Practice applies to personal health information (see definitions)

relating to identifiable or potentially identifiable data (see definitions), which is held by the Department of Health or the public health system. The Code applies irrespective of whether the person to whom the information relates is living or dead. For provisions for dealing with information about deceased persons see 7.7.

The principles guiding this Code apply to all personal health information irrespective of whether it is stored in paper or electronic form. Different formats will require different approaches and procedures though the underlying principles remain the same.

3.3 What is not covered?

The Code of Practice does not apply to:

- statistical or other aggregated information which does not contain identifiable or potentially identifiable information
- staff information such as personnel files
- information other than personal health information which may be considered sensitive such as tender documents and private hospital registration information
- information covered by public interest immunity such as documents considered by Cabinet.

These categories of information are covered by privacy guidelines in the NSW Public Service Personnel handbook[2], Circular 98/79 Principles and minimum standards for the development of health services codes of conduct[3] and the Purchasing and supply manual[4] for Area Health Services.

3.4 What clients/patients have a right to expect

The procedures established to protect information privacy in this Code of Practice extend to all persons who receive health care from the public health system (including the Ambulance Service).

Clients/patients can be assured that:

- their personal health information will be protected in accordance with the Information Privacy Principles (see Appendix 1)
- confidential information will be given to another person only if this is important for their health care or can be otherwise legally and ethically justified
- they are, subject to limited exceptions, entitled to access their own health records
- they will have the opportunity to opt out of proposals to link personal health information from different sources
- comprehensive clinical information will be available to their health

care providers to enable optimal care.

3.5 What data users have a right to expect

NSW Health is committed to ensuring that information which supports the provision of health care is readily available to authorised users, when and where it is needed and is delivered in a timely and efficient manner. Accordingly this Code of Practice aims to promote:

- the integrity of data, so that information is accurate, complete and up-to-date; information integrity is critical for quality client/patient care, evaluation of services, medical research and the maintenance of public health
- the availability of data, so that authorised persons who need information for legitimate health purposes have ready access to it; if clinical information is not readily available to providers of health services, the care or interests of clients/patients may be compromised
- the optimum use of data, primarily for the benefit of those clients/patients to whom the data relates but also for the general betterment of the health of the population of New South Wales through public health surveillance and medical research.

3.6 Information Privacy Principles

This Code of Practice is consistent with the Information Privacy Principles (IPPs), endorsed by the NSW Privacy Committee, which may be summarised as follows:

Principle 1: Collection of information must be lawful and fair
Personal information should only be collected for a lawful purpose directly related to a function or activity of the agency.

Principle 2: Informed consent
Personal information should normally be collected directly from the individual concerned. At the time the information is collected the individual should be advised why it is being collected, whether provision of the information is compulsory and who else will have access to the information.

Principle 3: Data quality
Agencies should take reasonable steps to ensure that the personal information they collect is relevant, accurate, up-to-date and complete and does not intrude to an unreasonable extent on the personal affairs of the individual concerned.

Principle 4: Data security
Agencies should ensure that personal information is protected by appropriate security safeguards from loss, unauthorised access or misuse.

Principle 5: Openness

Any person has a right to know whether an agency holds personal information about them and, if so:

* its nature and source
* the main purpose for which it is used
* the classes of persons about whom it is kept
* the period for which the information is kep
* the persons who are entitled to have access to it; and
* how to obtain access to it.

Principle 6: Access

A person has a right of access to personal information held by an agency, subject to exceptions of the *Freedom of Information Act* or other relevant law.

Principle 7: Correction of records

Agencies should make any corrections, deletions or additions to personal information to ensure it is accurate, up-to-date and complete. Agencies should, on request, add any reasonable statement a person wishes to see included in their record. Other recipients of the information should be informed about corrections.

Principle 8: Ensuring data quality before use

Agencies should take reasonable steps to ensure that information is relevant, accurate, up-to-date and complete before use.

Principle 9: Using personal information

Agencies should not use personal information for purposes other than for which it was collected except:

* with the consent of the person
* to prevent a serious threat to a person's life or health
* as required or authorised by law.

Principle 10: Disclosing personal information

Agencies should not disclose personal information to other parties except:

* with the consent of the person
* to prevent a serious threat to a person's life or health
* as required or authorised by law.

The recipient of the information can only use it for the purpose for which it was disclosed.

Principle 11: Sensitive personal information

Notwithstanding principles 9 and 10, information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life should not be disclosed by an agency without the express written consent, freely given, of the individual concerned, or authorisation under the law.

(The full text of the IPPs is at Appendix 1.)

4 LEGISLATION REQUIRING CONFIDENTIALITY

A number of existing Acts require people working in the NSW health system to maintain the confidentiality of information acquired in the course of their work. The requirements of these Acts are summarised below. It should be noted that the confidentiality provisions in these Acts, with the exception of section 17 of the *Public Health Act*, do not draw a distinction between personal and other information, but apply to any information acquired in the course of duty.

4.1 Health Administration Act 1982

The *Health Administration Act* covers any information which is provided or recorded pursuant to any Act in the health portfolio. It is binding on all persons working in the NSW health system. Section 22 contains the main confidentiality requirements.

Under section 22, information cannot be disclosed unless certain specified criteria are satisfied. These criteria cover:

- with the consent of the person to whom the information relates
- in connection with the administration of health legislation (ie. Where other legislation such as the *Public Health Act* authorises or requires disclosure)
- for the purposes of legal proceedings arising out of health legislation, eg. pursuant to a court order or subpoena
- 'with other lawful excuse' such as for example, orders under other court proceedings, assisting the police in investigating a specific criminal offence, or a lawful direction by the Minister or Director-General
- in other prescribed circumstances. Regulations currently exist to allow the Chief Health Officer to release epidemiological data and the Director-General to release other information for the purposes of research. Such data are only released to bona fide researchers and on condition that the confidentiality of data is maintained.

Clause 13 of the Health Administration General Regulation 1995, states that it is not an offence to disclose information covered by section 22 if:

- the information is epidemiological data; and
- the disclosure is made in accordance with the written approval of the Chief Health Officer; and
- that approval describes the information that is authorised to be disclosed and names the person or body to whom disclosure is authorised.

Information covered by clause 13 and which identifies an individual, may only be released by the Director-General, complying with the requirements set out in

clause 13(3).

The Act provides for a penalty of a fine of up to $1,000 or imprisonment for a term not exceeding 6 months.

4.2 Mental Health Act 1990

Section 289 of the *Mental Health Act* contains similar provisions to section 22 of the *Health Administration Act* (see 4.1). It relates specifically to information obtained in the course of duties performed under the *Mental Health Act* and is of particular relevance to people working in the mental health field.

The Act provides for a penalty of a fine of up to $5,000 for unauthorised disclosure of information.

4.3 Public Health Act 1991

Section 75 of the *Public Health Act* contains similar provisions to section 22 of the *Health Administration Act* (see 4.1). Under Section 75 a person who discloses information obtained in connection with the Act is guilty of an offence. The Act contains similar exemptions to those listed in the *Health Administration Act* and clause 81a of the Public Health Regulation 1991 allows the release of epidemiological data where there is written approval from the Chief Health Officer.

The most important confidentiality provision in the *Public Health Act* is section 17 which deals specifically with “HIV/AIDS related information”. Under the Act this means two things:

- the fact that a person has had or is going to have a HIV test; and
- the fact that a person is HIV positive.

Section 17 places strict limitations on the release of this information, which can only be disclosed:

- with the consent of the person to whom the information relates
- in connection with the administration of an Act
- under an order of a Court or a person authorised to examine witnesses
- to a person involved in the care or treatment or counselling of the person to whom the information relates, if required, in connection with that care.

The Act provides for a penalty of a fine of up to $5,000 for unauthorised disclosure.

4.4 Obligations of health professionals

Some health professional groups are registered under statute. This health professional registration legislation also provides a basis for clinical and professional standards and defines 'professional misconduct' or in some cases 'unsatisfactory conduct'. Breach of the confidence owed by a health care provider to a client/patient constitutes professional misconduct and may therefore be subject to disciplinary action.

In addition, health care workers and public health organisations can owe a common law duty of confidentiality to their clients/patients. This duty arises from the nature of the relationship between health workers and their clients/patients.

Health care providers may be sued in the civil courts by clients/patients for breaches of confidentiality. Damages will be awarded according to the injury or harm to a client/patient caused by the breach of confidentiality. Health workers should be aware however, that a common law action for breach of confidence will also recognise a defence that the disclosure was lawful where a statutory obligation or power exists to justify disclosure. Where a confidentiality obligation exists a client/patient may also, if aware that the duty may be breached, seek court orders to prevent the breach occurring.

Various professional codes of ethics also require that confidentiality of personal information be maintained. Although such codes do not have the binding authority of a statute, breaches may incur disciplinary action. More broadly, they are a reflection of the prevailing view of proper conduct among the health professions.

4.5 Health service codes of conduct

The Principles and minimum standards for the development of health service codes of conduct[3] have been issued by the Department to provide a framework for the development of local codes of conduct by health services. In line with Premier's Department requirements, codes of conduct aim to provide guidance for staff in relation to decisions, actions and general conduct in their employment. They promote a standard of behaviour which demonstrates respect for the rights of the individual and the community and maintains public confidence and trust in the work of the public health system.

The Principles cover a wide range of personal and professional behaviour including a requirement that all employees observe the confidentiality of personal and other official information.

5 ACCESS BY THE CLIENT/PATIENT

As a matter of policy, clients/patients are guaranteed a right of access to information about them held by public health organisations. They also have a right to access their health records under the *Freedom of Information Act* (see 7.4*)*. A charge may be made if copies are required (see the Patient matters manual[5] section 9 for details). See 5.6 for access in private health care facilities.

In some cases a decision may be made to give the information to a medical practitioner of the client/patient's choice rather than directly to the client/patient (see 5.5).

Clients/patients should be informed, as a matter of routine, about their rights to access their own records. This may be done in any way which is appropriate for the public health organisation, for example notices in waiting rooms, leaflets, explanatory paragraphs on admission/registration forms etc. (see Appendix 3). Any request for access should be noted on the record.

Access by clients/patients to their own health records is subject to the provisions set out below.

5.1 Dissenting comments

If a client/patient wishes to dissent from or add to his/her health record, he/she is entitled to do so. The client/patient's own comments should be attached as an addendum to the record on request, along with an explanation of the circumstances. Alterations to the record should not be made unless in accordance with 10.4.1.

5.2 Proof of identity

In all cases where access is granted, proof of identity is required. Two forms of identity should be sighted, such as driver's licence, health benefits card etc., preferably with a photograph.

5.3 Requests for specific information

Access should generally be provided by direct access, or viewing of the record on the organisation's premises. If the client/patient wishes to have copies of the health record made, charges as set out in the Patient matters manual[5] section 9 will apply. When copying records for legal purposes, employees should be aware of the requirements of the *Evidence Act 1995.*

5.4 Presence of health care provider

Clients/patients may request the assistance of a health care provider in interpreting the record. A health care provider or health information manager should always supervise access by a client/patient to his or her health records.

5.5 Circumstances where access may be refused

In circumstances where the treating health care provider considers access could be prejudicial to the physical or mental health of the client/patient (and this would be a rare occurrence), the health record should be referred to a third party such as an independent health practitioner. The health record plus the assessment should then be referred to the senior health care provider for review and a decision on whether the client/patient should be granted access to all or part of his/her record.

If access is not granted following the review, the client/patient should be advised that an appeal may be made to the Chief Executive Officer. The client/patient is also entitled to exercise their rights under the *Freedom of Information Act* (see 7.4).

Where access is granted but there remains a concern as to the impact the information may have on the client/patient, a written warning to this effect should be given to the client/patient, and a copy included on the record.

5.6 Access in private health care facilities

The licensees of private health care facilities are required, under the Private Hospitals Regulation 1996, the Day Procedure Centres Regulation 1996 and the Nursing Homes Regulation 1996 to:

- provide patients and former patients or their representatives or nominees with access to their clinical records
- ensure that personal information is not released without the consent of the patient or former patient or with other lawful excuse
- ensure that clinical records are stored securely.

Patients of private health care facilities have a right to:

- access their clinical records or request a copy
- be assisted by a qualified person to interpret the record
- have comments attached as an addendum if they disagree with information in the record.

Access may be refused if the licensee considers, on the advice of the treating health care provider, that access would be prejudicial to the patient's physical or

mental health, although this would be a rare occurrence (there are no grounds for refusing access to the record of a deceased person). The applicant may appeal to the Director-General against a decision to deny access.

6 AUTHORISED DISCLOSURE

6.1 Informed consent

Informed consent of the client/patient is acknowledged as one of the cornerstones of information privacy. Personal health information should not be disclosed without the consent of the person to whom it relates, except in the specific circumstances set out in this Code.

For consent to be valid:

- the client/patient must be legally competent, that is, be able to understand the nature and consequences of the proposed use of the information
- it must be freely given
- it must be informed, that is, sufficient information provided to allow a reasoned decision
- it must be specific.

The health care provider or organisation to whom information will be released should be specified and the information provided should be limited to that relating to the current episode of care. Access to information about an unrelated episode or to the full clinical history requires separate express consent.

Obtaining consent in advance where the condition requiring care has not manifested is not acceptable, as the client/patient will not be aware of who will be accessing the record or for what purpose.

6.1.1 Informing clients/patients

There is a need for clients/patients to be better informed about how their personal health information will be used. This should include an understanding of:

- who will have access to the information
- the reason why the information is collected
- whether collection of the information is voluntary or mandatory (though consent will not be required if mandatory, the patient/client should nonetheless be informed)
- how the information will be used
- any proposed disclosure of the information to third parties, and
- if relevant, that the information will be computerised.

Appendix 3 contains sample wording for a statement which informs clients/patients about the collection and use of their health information. This may be added to admission/registration forms, be produced as a separate leaflet or displayed as a sign.

If consent is not given, or if limitations are applied, this should be noted on the client/patient's health record and complied with when any application for access is made.

Some intended uses of the information will be self-evident, such as where it is collected by a health care provider solely for the purpose of providing treatment. We cannot assume however that consent exists for all possible uses or disclosures of personal health information.

6.1.2 Legal impairment

There should be an awareness that, in a small minority of cases, there will be a need to carefully assess the capacity of the client/patient to consent. A person is incapable of giving consent if they are incapable of understanding the nature and effect of the proposed use of information or incapable of indicating whether or not they consent.

Written consent must be obtained from the legal guardian of a client/patient who lacks mental capacity. Where there is no legal guardian, under the *Guardianship Act,* the matter should be brought to the attention of the Guardianship Board.

6.1.3 Minors

Where a client/patient is less than 14 years of age, consent for access to information must be given by the parent or legal guardian.

Where the client/patient is between 14 and 16 years of age, consent of the parent or legal guardian should be sought unless the client/patient indicates a strong objection. In this case, the treating health care provider should assess the maturity of the client/patient, in particular their ability to understand the consequences of their decision. If the health care provider assesses the person to be capable of properly deciding on the issue, then it is a matter for the client/patient. Otherwise consent of the parent or legal guardian should be obtained.

Where the client/patient is 16 years of age or over, they are considered by law to be capable of deciding on the access issue for themselves.

6.1.4 Serious threats to health

In accordance with IPP 10, in cases of emergency or when a client/patient is at serious risk, personal information may be disclosed for the purpose of preventing or reducing that risk.

6.2 Disclosure with legal authority

6.2.1 Obligations to warn for the protection of the community

There are a range of specific circumstances where a health care provider will be excused from breaching confidentiality, where he or she discloses information in order to protect the public. Some of these exemptions are established through statute, others through judicial interpretation of the law.

6.2.2 General 'duty to warn' to protect members of the public

Where a health worker becomes aware, in the course of managing a client/patient, that a risk to public safety exists, he or she will be excused from breaching confidentiality where he or she discloses information about this risk in order to protect the public. In this context 'public safety' includes instances where the risk is to a particular individual.

Health workers should be aware that the "duty to warn" is unlikely to arise in day to day case management and so disclosure on this basis will be a rare occurrence. In circumstances where a health care provider considers that a client/patient represents a risk to the public, they should carefully assess the level of risk before acting. It is advisable to discuss the situation with colleagues or a senior health care provider before acting.

6.2.3 Notification of public health risk for HIV

Under the *Public Health Act* strict limitations are imposed on the disclosure of information indicating a person's HIV status, and information that a person has undergone a HIV test. The general obligations in relation to the confidentiality of HIV information are set out in section 4.3 and more fully in section 9 of the Patient matters manual[5].

Staff should be aware however that the *Public Health Act* allows for the disclosure of information relating to a person's HIV status where the failure to provide the information could place the health of the public at risk. The disclosure provision is limited however and only allows notification of the Director-General of the Department of Health. It does not authorise disclosure to any other person.

If staff are concerned about a possible health risk relating to HIV or the behaviour of a HIV positive person, they should contact their local HIV co-ordinator or the AIDS and Infectious Diseases Branch of the Department of Health.

6.2.4 Obligation to notify police of certain information

Under the NSW *Crimes Act* there is an obligation for people who have information about serious criminal offences to notify the police. Section 316 of the Act requires a person to consider whether the information they have will be of 'material assistance' to securing the apprehension or conviction of an offender. If so, they are obliged to notify police. Failure to do so could lead to a conviction and the imposition of a penalty of up to two years imprisonment (see also 6.3.7).

A 'serious criminal offence' is an offence which attracts a penalty of five years imprisonment or more. Health workers should be aware that this covers offences such as drug trafficking, serious assaults, sexual assaults, murder and manslaughter. It does not cover minor possession offences or any offences under public health legislation.

6.2.4.1 Reporting of sexual assaults

Health workers should be aware that, in relation to the reporting of sexual assaults, the Interagency guidelines for responding to adult victims of sexual assault[6], jointly issued by the Department of Health, the Police and the Director of Public Prosecutions, establish appropriate protocols and procedures for all issues dealing with sexual assault. Health workers are referred to that policy for guidance on appropriate action.

6.2.5 Subpoenas

Compliance with a subpoena is required by law. The return date should be noted on receipt and the subpoena dealt with promptly by the officer designated to co-ordinate responses to subpoenas.

Where a client/patient whose health record has been subpoenaed is not named as a party to the proceedings before the Court, he or she should be notified by the public health organisation that the subpoena has been received and advised of the return date.

A subpoena may be challenged on a number of grounds including:

- abuse of process
- oppression (where the terms of a subpoena are excessively wide and imprecise)
- public interest immunity
- legal professional privilege.

If a health worker has concerns about the scope of a subpoena, he or she should consult their immediate manager and obtain advice from the health

service's solicitors if appropriate. See Circular 98/29 Subpoenas[7] for more information.

Care should be taken that documents outside the scope of the subpoena are not provided. If acceptable, copies should be provided and the original record retained by the organisation. Where originals are required, the records should be forwarded to the Court and a complete copy kept by the organisation.

Documents should be delivered to the Registrar or Clerk of the Court in question in a secure fashion (see Circular 98/29[7] for details). A receipt signed by the official receiving the record should be obtained which specifies the record number, date received and name of the Court.

6.2.5.1 Sexual assault and confidential communications privileges

Amendments made to the *Evidence Act* in 1997 established a sexual assault communications privilege, which creates a presumption that communications between a counsellor and a person who has been sexually assaulted, are **not** admissible as evidence. The onus is then on the accused to argue that the material would be likely to substantially assist in their defence and that the evidence could not be obtained from alternative sources.

Health organisations have special responsibilities in relation to challenging subpoenas which call for the production of documents containing sexual assault counselling communications. Any person who counsels clients/patients who have been victims of sexual assault or controls their records should be aware of their obligations not to give evidence or hand over documents without either:

- the client/patient's consent in writing; or
- a direction of the Court.

When a subpoena requesting sexual assault counselling records is received the client/patient and the relevant treatment unit should be contacted immediately.

The *Evidence Act* also gives judges the ability to exclude evidence of any confidential communication occurring in a professional health relationship where they are satisfied that there is a likelihood of harm being caused to the client/patient if the evidence is admitted and the nature of the harm outweighs the desirability of the evidence being given.

6.2.5.2 Sensitive records

Irrespective of whether grounds exist for challenging a subpoena, in the case of sensitive records such as sexual assault, drug and alcohol, HIV/AIDS, domestic violence, mental health, sexual health, genetics, IVF and artificial insemination programs, records of children considered to be at risk and records containing information about other persons, the facility should attach a letter requesting the Court to order that access be restricted and setting out reasons why the documents should not be produced in open court.

See Circular 98/29[7] for complete procedures regarding subpoenas.

6.2.6 Coroner

The *Coroner's Act 1980* requires notification to the Coroner of deaths occurring under certain conditions. Deaths associated with anaesthesia are also to be notified to the Special Committee Investigating Deaths under Anaesthesia.

Health records required for post-mortem examinations must also be provided to the Coroner. Where a post mortem is to be conducted the pathologist or medical officer conducting the post mortem should also have access to the health record. When health records are tendered to the Coroner, the treating health care provider should be notified.

See the Patient matters manual[5] section 19 for complete procedures regarding notifications to the Coroner and complying with a coronial summons.

6.2.7 Department of Community Services (DOCS)

6.2.7.1 Notification of suspected child abuse

Health workers are under a general obligation to notify the Department of Community Services of cases of suspected child abuse. This obligation is imposed on medical practitioners under section 22 of the *Children (Care and Protection) Act* and is extended to other health care workers under section 2.18 of the Patient matters manual[5]. For fuller information on reporting obligations refer to this section of the manual.

The *Children (Care and Protection) Act* contains the following provisions which protect the person notifying a case of suspected child abuse to the Department of Community Services:

- the notification shall not be held to constitute a breach of professional etiquette or ethics
- no liability for defamation is incurred by reason of the making of the notification
- the notification shall not constitute a ground for civil proceedings for malicious prosecution or for conspiracy.

See section 9 of the Patient matters manual[5] for procedures for notification of suspected child abuse cases.

6.2.7.2 Obligation to co-operate with DOCS

Obligations also exist under the *Children (Care and Protection) Act*, requiring disclosure of relevant information where action is pending against a parent or carer, or when the information is required to determine whether a child is in need of care. In the event information is required on this ground, police or community service workers should indicate the statutory basis on which they require the information.

Requests for such information should always be referred to the treating health care provider or senior health care provider. In such cases the consent of the parent or guardian is not required. Relevant information on the record of a parent of a child so suspected may also be released.

DOCS workers also have the power to request a medical examination of a child. When this occurs, any information obtained in the course of the examination may be disclosed to the Director-General of DOCS or a delegated officer, as the examination has been ordered under the authority of the *Children (Care and Protection) Act*.

6.2.7.3 Requests for information by parents

Where there is a request for access to a child's health record by a parent or guardian against whom an action in relation to child abuse may result, the treating health care provider may refuse access to that parent or guardian if it could be prejudicial to the physical or mental health of the child.

6.2.7.4 Access by the Child Death Review Team

The Review Team is responsible for reviewing child deaths which occurred in suspicious circumstances and may have resulted from abuse or neglect. Under section 104(3) of the *Children (Care*

and Protection) Act the Review Team has powers to obtain full and unrestricted access to relevant health records and to obtain copies on request. Requests from the Review team should be acted upon within 5 to 10 days of being received. See section 9 of the Patient matters manual[5] for detailed procedures.

6.2.8 Official Visitors

Under the *Mental Health Act* Official Visitors must be given access to any records or other documents requested by them relating to the care, treatment or control of patients or persons who are detained in psychiatric hospitals or subject to community orders.

6.3 Access by government authorities

A number of government authorities, both state and federal, have specific statutory powers to demand access to information. In circumstances where a request is made by an officer of an authority or government department for access on this basis, staff should check:

- the precise authority of the person requesting access, including reference to the section of the Act under which access is authorised
- the nature of the access requested, to ensure that only material relevant to the statutory demand is released.

Before supplying the information, written confirmation should be obtained and kept on file. Information should be restricted to the minimum required to satisfy the statutory requirement.

Where the consent of the client/patient to such access has not been obtained, attempts should be made to notify that such access has been given.

Some examples of common requests for access are set out below.

6.3.1 Department of Health officers

Inspectors carrying out their routine duties under the *Health Services Act*, *Public Health Act*, *Private Hospitals and Day Procedures Centre Act* or *Nursing Homes Act* all have statutory powers to obtain information. Inspectors carry written authorisations, under these Acts, which indicate the nature of their powers and confirm their authority to act.

6.3.2 Health Care Complaints Commission

Authorised officers of the Health Care Complaints Commission (HCCC) also have certain powers of entry. Authorised officers carry a written

authority under the Act which indicates the nature of their powers and confirms their authority to act. Authorised officers of the HCCC may only exercise their powers of entry with the consent of the owner or occupier or under the authority of a search warrant. These powers of entry include the rights to enter and inspect premises, examine, retain or remove equipment, require the production of records, remove them or take copies of them, require any person to answer questions or furnish information.

6.3.3 The Ombudsman

The Ombudsman is empowered to require health authorities to supply information where a formal investigation is being conducted under the *Ombudsman's Act*. No information should be provided without prior reference to the Department's Complaints Manager in the Executive Support Unit.

For further procedures relating to the Ombudsman see Circular 91/91 Ombudsman matters[8].

6.3.4 Department of Social Security

Under the *Social Security Act*, the Department of Social Security has the right to access information that may affect the granting or payment of a pension, benefit or allowance to any person, provided the request is in writing and notice is given under section 1304(1) of the Act.

6.3.5 Department of Foreign Affairs and Trade

The Department has agreed to provide to the Department of Foreign Affairs and Trade, relevant information relating to overseas students, in order to meet its obligations to them and their families.

6.3.6 Department of Veterans' Affairs

Under section 128 of the *Veterans' Entitlement Act* the Department is required to release to the Department of Veterans' Affairs relevant information relating to treatment received at any public health facility by Repatriation beneficiaries.

6.3.7 Police access

6.3.7.1 Authorised by client/patient

Where a client/patient has authorised the police to have access to information from his/her records, this should be supplied on the standard police form P190.

6.3.7.2 Not authorised by client/patient

Requests for information by the police should be dealt with by the treating health care provider or senior health care provider.

Generally, the information supplied should be limited to confirmation of identity and address. The only exception is where the police can confirm they are actively investigating the commission of an offence and that the information is 'essential to the execution of their duty'. In this case the information released should be limited to a general outline of the client/patient's condition and/or injuries, and confirmation of the client/patient's identity and address. Any other information may only be provided in response to a search warrant.

Requests from police should be in writing and the identity of the requesting officer (eg. badge number) noted.

6.3.7.3 Search warrants

Compliance with a search warrant is required by law and record keepers are advised that they should inform their immediate supervisor of any official demand for access to data.

6.3.7.4 Police interviews of clients/patients

Except in the case of declarations from dying clients/patients, permission to interview a client/patient should only be given (where the client/patient agrees), by the clinician, when the client/patient's medical condition permits.

6.3.8 Prison officers (access to medical records of prisoners)

The staff of the Corrections Health Service may disclose information relating to the medical history of a prisoner to a prison officer duly authorised by the Gaol Superintendent to investigate an incident or assault involving that prisoner. Corrections Health Service staff must, in these circumstances, complete the document entitled Corrections Health Service Incident/Assault form.

6.4 Notifications

Notification of certain information to authorised agencies as set out below is required.

- The *Public Health Act* requires notification of scheduled medical

conditions to the Department of Health.

- Under the *Registration of Births, Deaths and Marriages (Amendment) Act 1973* perinatal deaths must be notified to the Principal Registrar for perinatal deaths.
- The Department of Veterans' Affairs should be notified of the deaths of repatriation clients/patients.
- The Australian Drug Evaluation Committee should be notified of adverse drug reactions.
- The *Health Services Act* and the *Private Hospitals and Day Procedures Centres Act* require all hospitals and day procedures centres (public and private) to report inpatient information to the Department's Inpatients Statistics Collection.
- The *Public Health Act* requires notification to the Department of maternal and perinatal information for the Midwives' Data Collection.
- The *Public Health Act* requires notification of cancer cases to the Central Cancer Registry.
- Notification to the Department of birth defects detected in infants up to twelve months old is required for the Birth Defects Register.

For detailed procedures regarding notifications refer to the Patient matters manual[5] section 9.

6.5 Access authorised by a client/patient

A client/patient may authorise any third party, such as a relative, interpreter, medical practitioner, legal representative, employer, insurer or officer, to have access to his or her health record. Members of parliament making representations on behalf of a constituent are also required to have authorisation.

6.5.1 Conditions of access

Where a third party has been authorised to access a health record, proof of identity should be provided and the access supervised, as set out in 5.2 and 5.4.

6.5.2 Form and content of authorisation

The client/patient's authority should be in writing (not a photocopy, except in circumstances outlined in 6.5.4). It should be signed by the client/patient or their parent or legal guardian and should contain:

- full name of client/patient
- date of birth
- present address and, if different, address at the time of the health treatment in question
- date of written consent which should be less than three

months before access is sought
- details of the records/information in question
- range of dates for health treatment in question
- name of person being authorised
- the purpose for which the information is requested.

Photocopies of consent authorities are not sufficient unless they are from a client/patient's insurer, as set out in 6.5.4.

The precise authority of the person requesting access and the nature of that access should be checked to ensure that only relevant material is released.

6.5.3 Client/patient's legal representative

Where the client/patient's legal representative has been authorised to view the complete health record of a client/patient, the health care facility should make such access available within facility premises. If requested, the facility should attempt to provide photocopies. Such photocopying is to be at the expense of the legal representative and charged at current rates (see the Patient matters manual[5] section 9 for details).

Similar access should also be provided to any medical practitioner nominated and authorised by the client/patient.

6.5.4 Client/patient's insurer

Where a request is made for information related to an insurance or compensation claim, a photocopy of the insurance application or compensation claim form, signed and dated by the client/patient, containing the client/patient's consent to disclosure, is sufficient authority for the release of a medical report or summary of injuries. Other information should not be provided without the clearly documented written consent of the client/patient.

Details of charges for medical reports and copies of health records are detailed in the Patient matters manual[5].

6.6 General practitioners, external providers and facilities

Clients/patients should be aware that, on discharge, it is normal practice to provide their GP's and other providers involved in ongoing care, for example, community nursing, early childhood services, with a discharge summary.

With the exception of the discharge summary, release of client/patient information

to health care providers or organisations outside the public health system requires consent (see 6.1). In all but emergency cases the consent should be in writing (see 6.5.2).

7 OTHER ACCESS

7.1 Health care providers

Other than in the circumstances set out below, health care providers have no greater right of access than any other third party, and access for any other purpose must be sanctioned by one of the exceptions listed in this Code.

Any health care provider in the public health system currently involved in the continuing care or treatment of a client/patient may access the health record of that client/patient. However as a matter of principle, sensitive categories of health records such as sexual assault, drug and alcohol, HIV/AIDS, domestic violence, sexual health, mental health, genetics, IVF and artificial insemination programmes and records of children considered to be at risk, should not be accessed by health care providers who are treating the client/patient for other reasons, unless consent is obtained (see also 8.1).

Clients/patients should be made aware that their contract for treatment is not with an individual health care provider but with the public health organisation from which they are receiving treatment. Admission and registration forms should include a statement that access to a client/patient's health record will be available to the client/patient's treating health care providers within the public health system, both inside and outside the public health organisation (see Appendix 3).

7.1.1 Students

Student health professionals enrolled in recognised teaching institutions may have access to health records with the approval and under the direction of their supervisor if that access is sought in respect of their education program at the health facility. Clients/patients may refuse to have a student participate in their treatment.

7.1.2 Conclusion of care

When an episode of care concludes for whatever reason (including the death of a client/patient), the right of access by a health care provider to the health record is normally terminated at the same time, although access may still be authorised for purposes other than client/patient care, such as clinical audit or research.

7.1.3 Records of family members

Requests by health care providers for access to health records of members of a client/patient's family cannot be treated as exceptions to the rule and must be accompanied by the written consent of the person to whom the record relates.

7.2 Quality assurance and audit

Members of, or persons directed by, quality assurance committees or peer review committees, or persons undertaking audit activities, including clinical audit, may have access to health records which directly relate to these activities. Practical measures should be taken to protect the confidentiality of identifiable data and individual health records should not be accessed where alternate records are available, and if accessed, where possible this should be undertaken on a sample basis.

7.3 Research

Proposals for research, surveillance or statistical projects for which access to personal health information is required should comply with the NHMRC Guidelines for the protection of privacy in the conduct of medical research[9], which specify that a Research Ethics Committee must consider every research project which may breach one of the Information Privacy Principles. For the project to be approved, the REC must consider that the public benefit of the research outweighs to a substantial degree the public interest in observing the IPPs (see also 11.4).

When personal health information is to be used for research purposes, this should normally be disclosed to the client/patient and consent obtained. If disclosure or the gaining of consent is not proposed, reasons and justification should be given and accepted by the REC.

7.3.1 Direct contact or identifiable data

Where a research proposal requires clients/patients to be contacted directly by the researcher, or where identifiable or potentially identifiable information is requested, the informed consent of the client/patient should normally be obtained through the treating health care provider or the senior health care provider prior to access being granted. If this is not proposed, reasons and justification should be given and accepted by the REC.

7.3.2 Nature of access for researchers

Where access is granted under these provisions, health records are not to be removed from the public health organisation, nor are they to be copied, or, in the case of electronic records, downloaded.

7.4 Freedom of Information

Where an application for access under the *Freedom of Information Act* is made

by a third party, staff must ensure that the request is referred to the FOI officer as soon as possible to ensure the matter is dealt with promptly. For charges applying to FOI requests see the Patient matters manual[5] section 9.

For treatment of FOI requests by adoptees seeking to identify their natural parents see the Patient matters manual[5] section 9.

7.5 Fundraising and public support campaigns

7.5.1 Informed consent

Consistent with the principle of informed consent, access to personal health information for the purpose of fundraising or gaining public support will not be granted unless such access was specifically consented to by the client/patient at the time of collection. The form of the consent request should be approved by the relevant REC.

Client/patient details may only be included on lists compiled for fundraising and public support campaign purposes with their specific consent. The right to withhold consent should be made clear at the time such consent is sought.

Clients/patients have a right to withdraw consent and to have their names and addresses removed from any lists held. To this end:

- direct mail should contain a statement of the addressee's right to have his/her name removed from mailing lists
- correspondence should clearly display the name and full address of the sender.

Committees involved in fundraising and/or public support campaigns should ensure that names and addresses are deleted from mailing lists promptly when requested.

7.5.2 Limits on what information may be used

The information which may be released with consent is limited to name and address. Information relating in any way to a client/patient's health status is not to be included in information made accessible for fundraising and public support campaigns.

7.5.3 Use of mailing lists

A mailing list should not be used for any purpose other than that for which it was compiled unless further consent is obtained from each person on that list. Mailing lists should be accurate, complete and up to date. When

no longer current, lists should be properly disposed of (see 12.3.3 and 12.4.2).

A mailing list should be securely stored and should remain at all times in the custody of the committee which originally compiled the list. A member may not have access to mailing lists or any personal health information held by that committee once they have ceased to be a member of the committee.

Committees are not to release to or exchange with any third party, lists containing personal health information.

7.5.4 Organisations with a commercial interest

Information regarding clients/patients must not be provided to organisations which may have a commercial interest in such information, even though it may be sought ostensibly for the purpose of offering assistance or advice.

7.6 Information sought by adoptees

Any application by an adoptee for access to birth-related information should be referred to the Family Information Service of the Department of Community Services. See the Patient matters manual[5] section 9 for full procedures.

Provided the identity (or information that may assist in identification) of the biological parents is withheld, information from the health record may be released on receipt of an authorised request from the Department of Community Services.

Where a request is received from other than the Department of Community Services, the facility should contact that Department to establish the bona fides of the inquirer before releasing the information.

To prevent matching of adopted persons or adoptive parents with biological parents in records, copies of correspondence should be kept physically separate from the biological parents' records.

7.7 Deceased clients/patients

In the case of a deceased client/patient's records, access may be granted to the next of kin as shown in the records. Written consent for access by a third party is to be provided by the next of kin as shown on the records, or the executor or administrator of the estate. Next of kin may include homosexual partners. In the event that there is no next of kin shown on the records, or the application is made

by a person not listed as next of kin, the applicant can be requested to apply under the *Freedom of Information Act*.

Any decision to disclose material held on a deceased patient should also have due regard to any view expressed by the patient to health workers prior to death, either in writing, or as recorded on the patient's medical file.

7.8 Government Insurance Office

Co-operation is to be afforded where the public health organisation's public liability insurer is the Government Insurance Office. Information and/or access to the relevant health record may be given to the solicitor for the GIO when acting on behalf of a defendant public health organisation in cases covered by the Master Public Liability Insurance Policy (Treasury Managed Fund). Such access does not require authorisation from the client/patient. The senior health care provider should be informed of such requests.

7.9 Media

7.9.1 Informed consent

No information about a client/patient should be released to the media without the informed consent of that client/patient. In addition, if the request includes requests for clinical or other information, these should be referred to the senior health care provider.

If the client/patient is conscious and can communicate, he/she should be asked whether information may be given. If the client/patient is not conscious the next of kin should be asked whether information may be given. The client/patient's or next of kin's decision is final.

Any decision to disclose material held on a deceased patient should also have due regard to any view expressed by the patient to health workers prior to death, either in writing, or as recorded on the patient's medical file.

7.9.2 Responsibility for media liaison

All media inquiries should be directed to Health Public Affairs Media Issues Management. A designated Media Liaison or Public Affairs officer should always be the first point of contact for the media. A media Liaison Officer from the Department is available at all times via the on call 24 hour media pager. Every Area Health Service also has an on call Media Liaison Officer.

7.9.3 Accident victims

Information released about accident victims should be limited to the

number of casualties, sex, approximate age and whether injuries are critical, serious or minor.

7.9.4 Information about medical practitioners

Medical news regarding a client/patient should not refer to a medical practitioner in private practice.

If information is released to the media an assurance should be sought from the facility concerned that the name of the client/patient's treating medical practitioner will not be published.

7.9.5 Tapes or images of clients/patients

A client/patient should not be photographed, or recorded on videotape or audiotape unless:

- the client/patient requests this or agrees in writing; and
- the opinion of the treating health care provider is that the client/patient's condition will not be jeopardised.

The client/patient should be informed about the purpose of the tape or image eg. therapy, health promotion, publicity etc.

7.10 Inquiries about clients/patients

A public health organisation may neither confirm nor deny the current or past presence of a person, unless the inquirer already knows that the client/patient is present. If staff are satisfied that this is so, and unless they believe that, in the circumstances, to do so would be contrary to the interests of the client/patient, they may release details of the ward. All other inquiries from family and friends should be referred to ward staff.

Where a client/patient requests that no information at all be released, or that information be released only in certain circumstances, such as in an immediate post-operative period, this request should be complied with and should be indicated on any client/patient lists held by the inquiry section.

7.10.1 Other safeguards for Inquiries Sections

Organisations should ensure that any client/patient lists held by inquiries sections do not include diagnosis and are kept out of view of the public.

Where possible, wards should be identified by name, letter or number rather than by specialty (eg. Ward A instead of psychiatric ward, colorectal unit etc.).

7.11 Health examinations of school children

Parental permission for health examinations of school children is usually recorded by the parent's signature on the school health card following a statement of consent to the examination. The results of vision and hearing tests and other health findings cannot be communicated to teachers or recorded on the Education Department Pupil Record Card unless additional consent is obtained or this was provided for in the original consent advice.

7.12 Organ/tissue transplants

In order to protect the privacy of grieving relatives of a recently deceased donor, it is not permissable to disclose any information which could enable the identification of the donor of a transplanted organ or tissue. Issues relating to the disclosure of information in such cases are comprehensively dealt with under Section 37 of the *Human Tissue Act 1983.* Under this provision the identity of the donor or recipient of transplanted tissue (whether living or deceased) must not be disclosed except in the following circumstances:

- with the consent of the person to whom the information relates
- in connection with the administration or execution of the *Human Tissue Act 1983*
- in connection with bona fide medical research which has REC approval
- for the purposes of any legal proceedings or reporting of such proceedings
- with other lawful excuse.

8 SPECIAL INFORMATION CATEGORIES

8.1 Sensitive records

Although all personal health information should be considered sensitive, there is an expectation in the community that certain categories of highly sensitive information which are potentially stigmatising should be treated with particular care. Clients/patients of certain services such as sexual assault, drug and alcohol, HIV/AIDS, domestic violence, sexual health, mental health, genetics, IVF and artificial insemination programs and children considered to be at risk, have special needs due to the sensitive nature of this information. The client/patient may indicate that their information regarding a particular condition is particularly sensitive. Examples of sensitive information include sexual assault, genetic testing etc. Care will be taken to ensure that access to the records of these clients/patients is strictly controlled (see also 7.1).

8.2 Aboriginal health information

8.2.1 Special characteristics

Health information relating to Aboriginal peoples has particular privacy needs. In addition to protecting the privacy of individuals there is also a need to safeguard the privacy of Aboriginal communities, which gives rise to the notion of community privacy.

In the past, information has been used for purposes which have not directly benefited and have frequently been damaging to Aboriginal peoples. For example, some information may be open to negative interpretations which have the potential to stigmatise Aboriginal peoples and fuel discriminatory community attitudes.

Another problem arises in small remote communities where it may be possible to identify individuals on the basis of very limited information, for instance, an uncommon diagnosis. This problem is not limited to, but is particularly common among Aboriginal communities.

8.2.2 Memorandum of Understanding

The NSW Aboriginal health information Memorandum of Understanding[10], developed jointly by the NSW Department of Health and the NSW Aboriginal Health Resource Cooperative, aims to provide a framework of ethical and culturally sensitive protocols for the collection and use of health data on Aboriginal and Torres Strait Islander peoples in New South Wales. The Memorandum sets out eleven guiding principles which support the objectives of self-determination and community control of

information, and supplement national and state policies, protocols and guidelines for the collection and use of Aboriginal health information.

The Memorandum is based on the recognition that Aboriginal peoples have rights and responsibilities of ownership regarding their health information. Coverage is not restricted to personal health information but, consistent with the notion of community privacy, also encompasses de-identified and aggregated information which includes Aboriginal samples or population groups.

8.2.3 Individual and group consent

In addition to individual consent, collective consent should be obtained from Aboriginal communities or community-controlled health services for the collection and use of health information about Aboriginal groups or communities. Such consent should be documented and dependent on compliance with the terms of the Memorandum.

8.2.4 Use of information

Requests for access to Aboriginal health information must demonstrate compliance with the terms of the Memorandum, as determined by RECs and the SHCEC, and information users must agree in writing to adhere to its terms. It is recommended that such requests should also be referred to the NSW Aboriginal Health Resource Cooperative Ethics Committee for consideration and advice.

For more detailed information on the collection, management and use of Aboriginal health information see the NSW Aboriginal health information Memorandum of Understanding[10].

8.3 Genetics information

The recording of genetic information about clients/patients raises specific information privacy problems. More detail on genetic information may be found in the Ethical code governing the provision of genetics services[11].

8.3.1 Predictive testing

The results of predictive or presymptomatic testing generally relate to healthy people but may indicate risk of developing a disorder in later life. Results are not necessarily predictive of age of onset or severity of the condition. Predictive test results may raise specific privacy issues with regard to access by third parties such as insurers and employer

8.3.2 Shared implications

Genetic information often has implications for people other than the individual client/patient receiving treatment, because genetic disorders are family health problems. A diagnosis in one family member may mean that other members are also at risk. Two examples of the ethical dilemmas which may arise with regard to information privacy are:

- A genetic test on an individual may reveal information about the health status of another family member who may choose not to know it. How and to what extent should this person's choice not to know be safeguarded?
- A person may wish to know genetic information about another family member for the purpose of making important life decisions such as whether to become pregnant. The other person may be unwilling to reveal the information. How should the conflict between each individual's rights be resolved?

It should be recognised that as a general principle, when disclosure of genetic information would allow early detection or effective treatment of a condition or affect important life decisions for other family members, the client/patient's right to confidentiality does not change, but the interests of others may also raise ethical concerns. Where a health care provider anticipates a situation where information will be obtained from a client/patient which may be of interest or potential benefit to other family members, he or she should discuss this with the client/patient prior to treatment being commenced or as part of protocols for ordering tests. Through counselling, individuals should be encouraged to accept their own responsibilities with regard to the information needs and rights of others.

8.3.3 Tissue samples

Stored tissue samples are a source of DNA which has the potential to yield considerable information about an individual. When tissue samples are stored:

- informed consent should be obtained
- the purpose for which storage is undertaken should be specified
- they should generally not be used for a purpose other than that for which they were collected without client/patient consent or for research approved by a Research Ethics Committee.

8.3.4 Genetics records

The health record of a genetic client/patient often includes a family tree with information about the health status of other relatives without their

knowledge or permission. For this reason genetics records should be stored securely and preferably separately.

Health records relating to a genetics diagnosis should be held indefinitely because of the potential value of family health tree information to other family members, particularly in following generations.

8.3.5 Genetic registers

Data from genetic registers should be collected, held and released in accordance with the NHMRC Guidelines for the use of genetic registers in medical research[12].

9 GENERAL SAFEGUARDS FOR PROTECTION OF PERSONAL INFORMATION

9.1 Transmission of information

Timely interchange of relevant information between the public health sector and community-based health care providers, notably GPs, is essential for optimal co-ordination of client/patient care. But while it is important to ensure that GPs have the information they need to care for clients/patients, this must be achieved in an environment where informed consent (see 6.1) and adequate privacy protection procedures are observed.

9.1.1 Phone, Fax and mail

The following basic procedures should be observed when transmitting personal health information to GPs and other authorised parties outside the public health system:

- No personal health information, including admission and discharge dates, should be given over the telephone unless it has been established that the caller has legitimate grounds to access the information and can give proof of identity.
- Only those authorised by the public health organisation should give client/patient information by phone; it is a matter for local determination which health workers should be so authorised.
- No personal health information about anyone except the caller should be left on voice mail.
- Fax machines used for transmission of personal health information should be secure; for example they should be located so that only persons granted access can access documents.
- Fax cover sheets should carry an appropriately worded privacy warning. See Appendix 2 for sample wording.
- Mail should be marked ‘Confidential: Attention ...’

9.1.2 Pathology test results

Transmission of pathology test results should comply with the National Pathology Accreditation Advisory Council’s Guidelines for data communication[13], which set standards for laboratory practice in relation

to electronic transfer of pathology data.

9.1.3 E-mail

When personal health information is sent by E-mail within the public health system, client/patient identifiers should be:

- removed if not essential; or
- encrypted; or
- sent separately from other information with link numbers or codes.

Only authorised individuals should receive personal health information by E-mail and are not permitted to forward such information; separate access for each individual will need to be authorised.

Any requests for transmission of personal health information by E-mail should be cleared by the data custodian (see 11.3.6) if the information requested is from a data collection.

If misdirected E-mail is received, the receiver should delete immediately and promptly inform the sender. The receiver should ensure that any backup or system copies are also deleted. The information should not be printed.

9.1.4 The Internet

It is acknowledged that the Internet is an efficient and cost-effective way of transmitting data between the public health system and authorised health care providers in the private sector. However it must also be recognised that there is community concern about some aspects of its use. It is essential to ensure that the privacy and integrity of personal health information transmitted via the Internet is protected to a high level by appropriate policies and procedures encompassing both administrative practices and data security. The broad guidelines set out below represent minimum standards for Internet transmission of personal information between the public health system and authorised external users.

9.1.4.1 Administrative procedures

Technological safeguards can provide a high standard of protection against security incidents such as system intruders. However such incidents are less likely to be the occasion of a breach than a lapse in good practice involving human factors.

9.1.4.2 Data security

The level of data security should be adequate to ensure:

- Data privacy - the message is encrypted in whole or in part so that interceptors cannot read its contents.
- Message content integrity - the message received by the recipient is exactly as transmitted by the sender and has not been tampered with either accidentally in transit or intentionally by an infiltrator.
- Non-repudiation of message content - the sender cannot deny being the source of a message nor can the recipient deny receipt.

9.1.4.3 Standards

The trend is towards the use of a Public Key Infrastructure Framework to ensure acceptable data security when transmitting information across an open network such as the Internet. Public key infrastructure involves encrypting or scrambling data at one end and unscrambling it at the other using paired keys to encrypt and decrypt.

The following processes should conform to a generally recognised standard such as Standards Australia's PKAF (Public Key Authentication Framework):

- message authentication, validation and non-repudiation encryption algorithm
- establishing user identification and authentication
- management of encryption key generation, distribution and storage
- registration and certification processes.

9.1.5 Telehealth

The primary objective of telehealth is to enhance access to and equity of health services and resources for residents of both metropolitan and country areas of New South Wales by enabling real time, remote clinical consultation and more efficient transmission, storage and sharing of client/patient information.

Because telehealth is in its infancy in the Australian public health system the privacy, confidentiality and security issues surrounding its use continue to be debated. Consideration needs to be given to the specific circumstances arising from the use of image transfer and clinical consultations conducted by videoconference before a NSW Health policy can be finally agreed.

The broad principles set out below should be observed in the interim.

9.1.5.1 Informed consent

Informed consent of the client/patient, as set out in 6.1, should be obtained before any video consultation or videoconferencing is undertaken.

Clinical guidelines should specify who is permitted in each room during a video conference. Clients/patients should know exactly who is sitting in on the session, and should be introduced to all people who will be present at the remote site and advised that the consultation may be terminated at any time.

9.1.5.2 Health record

Clinicians' notes must acknowledge that the consultation was conducted using videoconferencing technology and note any disruptions which occur in the course of the consultation.

9.1.5.3 Taping

Note that for the purposes of the trial implementation of telehealth in New South Wales taping of sessions is not permitted for clinical, administrative or educational purposes.

9.1.5.4 Security

Video equipment and telecommunications lines used for telehealth should be protected by appropriate security measures as set out in Section 12.

9.1.5.5 Video conferences

For clinical consultations conducted by video conference equipment is to be set up so that the image received is the same as the image transmitted to ensure that clients/patients know exactly what is being seen by people at the other end of the link.

There will need to be strict local protocols to determine who is permitted in each room during a video conference and to ensure that all participants know exactly who is viewing the session and give consent.

9.2 Printing and copying

The more copies of personal health information that exist the more likely it is that a breach of privacy may occur. For this reason paper records containing personal health information should not be copied unless it is essential to do so. Where practicable, identifiable information should be blocked out on the copied record.

When printing documents containing personal health information, the person printing should personally remove the document from the printer. If personal health information is printed regularly, consideration should be given to siting a dedicated printer in a secure area. This would minimise the chances of inadvertent access by unauthorised people and counteract the danger of print jobs being lost in large print buffers.

9.3 Training and demonstrations

The anonymity of clients/patients should be maintained during case presentations, consultations with other health care providers, research activities and at seminars and conferences. Fictitious data should be used for all training and demonstration purposes. Use of photos, slides and other visual aids which allow identification of individuals should not occur unless the material is of critical importance and the consent of the client/patient has been obtained.

9.4 Conversations, unattended documents

It is important to ensure that client/patient information is not discussed in public areas such as corridors or lifts or indeed anywhere it is likely to be overheard. Likewise, care should be taken not to leave documents containing personal health information on work benches or anywhere they may be visible to unauthorised people.

9.5 Visibility of screens

Computer screens in emergency departments, admission and outpatient areas and other public areas should, where possible, be so placed that they cannot be seen other than by the staff member entering the information. If left unattended, no information should be left on the screen. Screen savers should be used where possible to reduce the chance of casual observation.

9.6 Use of interpreters

Clients/patients whose preferred language is other than English should be informed in their own language of their rights to access their health records.

Professional interpreters must be made available and the decision to use an interpreter should rest with the client/patient. This is a particularly important requirement where sensitive health information is involved (see 8.1). However health care providers may need to request the services of an interpreter if they have difficulty understanding a client/patient or are unsure about whether the client/patient has understood information given to them.

When collecting information or seeking consent for the use of data, a professional interpreter should be used to ascertain the wishes of the client/patient and obtain informed consent if appropriate.

Interpreters are obliged to keep confidential any information they may access in the course of their duties.

See Circular 94/10 Standard procedures for the use of health care interpreters[14] for details on the use of health care interpreters.

10 PROCEDURES FOR HEALTH RECORDS

10.1 Scope of this section

Health records may include a range of information including a client/patient's medical history, test results, clinical records, progress notes, nursing care notes and information from other providers such as pathology reports. In mental health organisations they often contain detailed family histories, clinical assessments and prognosis, observations by health care providers about the client/patient's personality and details of treatment given.

Health records are the major source of personal health information in the public health system and are covered by most provisions in this Code. This section deals specifically with administrative control of health records and with the particular privacy issues which arise in relation to community health and electronic health records. The Patient matters manual[5] section 9 contains complete policies regarding health records, and should be referred to for guidance on matters which fall outside the scope of the Code.

10.2 Administrative responsibility

It is the responsibility of the record keeper to ensure compliance with those provisions of this Code of Practice which apply to health records.

10.3 Documentation of information released

Details concerning the release of any personal health information should be documented in the client/patient's health record.

10.4 Quality of health records

The health record should be sufficiently detailed and comprehensive to:

- provide effective communication to health care providers
- provide for a client/patient's effective, continuing care
- enable evaluation of the client/patient's progress and health outcome
- retain its integrity over time.

Because the primary purpose of keeping health records is to enable better client/patient care, it is important that the information in the records is current, clear, accurate, complete and readily available. A number of documentation models exist and practices may vary according to local needs. Whatever model or method is used, the health record should be clear and comprehensible to

others.

10.4.1 Accuracy and completeness

To ensure that the health record is accurate and complete:

- information should be recorded at the time of consultation or procedure or as soon as it becomes available
- each entry should be clearly dated, with time of day where necessary
- the treating health care provider should periodically review the record for correctness
- each entry should be signed by the health care provider and their designation stated; name and designation should be clearly legible
- alterations or deletions should not be made; original incorrect entries should not be erased but lined through so the original entry remains readable, and such action should be explained and signed
- there should be an audit trail for electronic records.

For detailed procedures regarding accuracy and completeness of health records see section 9 of the Patient matters manual [5], or the Medical Practice Regulations 1998.

10.5 Control of health records

Control over the movement of records is of the utmost importance. An adequate record tracking system, tailored to local needs, is essential to facilitate prompt record location and ensure that client/patient care does not suffer and that privacy is not breached.

Systems for transporting health records within an organisation should be well supervised to ensure that the records are not accessible by unauthorised persons.

No document from a health record should be removed from that record without being replaced by a tracer note. The tracer should specify document destination and date document was removed. The tracer should remain on the health record until the document is returned.

No health record should be removed from its home location (ie the Health Record Department) without the following details being recorded in an appropriate system:

- health record number
- client/patient name
- destination/location of the health record
- person responsible for/in possession of the health record

- date health record was removed.

Refer to the Patient matters manual[5] section 9 for complete procedures relating to record control.

10.5.1 Removal

Records should be kept under adequate security and only removed from the public health organisation upon a court subpoena, statutory authority, search warrant, coronial summons (see the Patient matters manual[5] section 9) or order of the Director-General.

Whenever the original of a major health record leaves an organisation, a copy of that record should, where possible, be made beforehand and kept by the organisation.

10.5.2 Transfer

If it is necessary to transfer a record outside the organisation, it should be transferred under seal, marked 'confidential' and where possible sent by courier.

10.5.3 Storage, archiving and disposal

Record disposal should take into account the type of information contained in a record and possible future demand for it as well as the needs of individual public health organisations. In particular the following should be considered:

- use of records for client/patient care, medico-legal purposes and research and teaching
- archival value
- provisions of the *Evidence Act 1995* and the *Statute of Limitations;*
- available storage space
- relevant provisions of the State Records Act 1998.

Similar standards for maintaining privacy and security should be maintained for records in archival or secondary storage as for records in current use. See the Patient matters manual[5] section 9 for complete disposal schedules for various classes of organisation and record.

10.6 Health facility closures

When a facility is closed each responsible unit should create a file that includes details of:

- records or documents destroyed
- documents retained
- documents transferred to other locations
- officers who undertook closures.

See the Patient matters manual[5] section 9 for procedures to be observed on the closure of a health care facility.

10.7 Community health records

Comprehensive procedures for health records at community health facilities may be found in the Health records and information manual for community health facilities[15]. It should be noted however that procedures for community health records will be substantially affected by the introduction of the Community-Based Health Information System (see 10.8.1) within the next two years.

10.7.1 Group houses/hostels

Comprehensive health records of clients/patients residing in Ward-in-a-house, group houses or hostels should continue to be maintained and stored at the nearest community health facility.

The non-institutional nature of group houses and hostels may pose particular threats to the confidentiality of personal health information and special precautions should be taken to ensure that client/patient privacy is maintained. Records should be stored in a secure place, inaccessible to clients and visitors. Records maintained and kept at the home/hostel should be limited to:

- registration book: content may vary but should include identification data and referrals accepted and refused
- day book
- card index or mini-file: should include identification data, referral information and medication details.

10.7.2 Group sessions

Individual client/patient intake forms (or equivalent) should be placed behind a chart divider to separate them from the group form and protect the privacy of each client/patient.

10.7.3 Family records

In the case of family consultations, information on other family members may be recorded in the health record of the family member who is the client/patient. Extreme care should be taken to safeguard the privacy of

other family members.

Where release of information on an individual has been appropriately authorised (see 6.1), care should be taken to ensure that only information relating to the specific episode indicated by the individual client/patient is released.

10.8 Electronic health records

Full electronic records allowing direct entry of data by clinicians are currently in use in only a very limited way in New South Wales. Imaging systems where entries are written by hand and subsequently scanned in but which do not allow writing to or altering of the record are in somewhat wider use, mainly for storage and archiving purposes. Some preliminary principles are set down here in acknowledgement of the likelihood that use of electronic records and imaging will become more prevalent.

Electronic records differ from paper records in ways which warrant special consideration. Firstly, it is possible to have a number of copies of a single electronic record at different sites, giving more people access. Secondly, it is possible to control access to an electronic record in a way that is not possible with a paper record.

10.8.1 Community-Based Health Information System

The Community-Based Health Information System (CBHIS) which will support care to community health clients including providing electronic documentation of care and treatment, will be implemented from early 1999. Standardised security and access procedures are currently being developed. Clients will have the option of registering anonymously as a privacy safeguard.

10.8.2 Evidence Act

The *Evidence Act 1995* does not preclude electronic records being used as evidence unless their veracity can be questioned. To minimise the possibility of records converted from paper being open to challenge, the equipment and scanning processes must be capable of scanning to 100% accuracy with no possibility of corruption or manipulation of images. Control processes need to be implemented to ensure that images cannot be altered between scanning and storage or while stored. The question of standards for hardware and software systems and telecommunications also needs to be addressed.

10.8.3 Training

Health care providers must be able to access and use electronic records properly. Appropriate education and training should be provided. Education will also be needed to inform both client/patients and health care providers about their rights and duties in relation to the electronic record.

10.8.4 Accountability

Information technology staff need to have some form of control over electronic records. Implementation of access rules and some degree of control will pass from health care providers and health information managers to system staff. System staff are bound by this Code of Practice and should sign an acknowledgement of this. To ensure the integrity of electronic records there is a need to specify accountability for the system which delivers the record and for its processing. Failsafe backup will be required in case of disaster.

The treating health care provider, as the only category of person entitled to make an entry in the health care record, is accountable both for the quality of that record and the care that has been documented.

10.8.5 Access and quality control

The area over which the electronic record is available is significant, ie. individual facility, campus or area health service. The broader the system the tighter network and access controls will be needed. Individual user names and passwords should be used rather than generic ones for staff category.

Where the electronic record system covers multiple facilities, the records may contain a mix of entries from different sources or partial copies of records from other facilities. The ability to maintain a single, logical record in this situation is critical. This can be achieved through various means such as appropriate labelling of each transaction and adequate version control. Identification and authentication of the person making the entry is important (see 9.1.4.3).

Electronic records should meet the same quality criteria as paper records (see 10.4). When amendments are made to clinical information the original data should be retained.

10.8.6 Client/patient access

It is important to ensure that the right of client/patients to access their own records is not compromised by the introduction of electronic

records and resulting changes in retention and storage procedures. Adequate viewing and copying facilities should be readily available.

11 DATA COLLECTIONS

11.1 Reporting of information to the Department

Because of the particular characteristics of information held in data collections they have been separately addressed in this code. Statistical information and other data are submitted to the Department for inclusion in around 100 centrally maintained data collections. Other data collections are maintained and administered by area health services.

Data submitted to the Department should be stripped of identifiers except in special cases where required by law or approved by the Chief Health Officer or the Director-General (under the Health Administration regulation), where identification is necessary for epidemiological purposes.

11.2 Legislative mandates for collection and disclosure of data

The Department has a duty under a range of state legislation administered by the Minister, such as the *Public Health Act 1991*, the *Health Administration Act 1982*, the *Food Act 1989*, the *Private Hospitals and Day Procedure Centres Act 1988* etc., to collect certain information for regulatory, administrative, epidemiological and public health purposes. The Register of health data collections[16] lists all collections administered from central administration, such as the Midwives' Data Collection and the Inpatient Statistics Collection, and specifies which data is collected in accordance with legislation.

In addition, other legislation such as the *Public Finance and Audit Act 1983* and State/Commonwealth agreements such as the Medicare Agreement and the National Health Information Agreement require that certain data be made available for authorised purposes.

11.3 Administrative responsibility

11.3.1 Data Administrator

Overall responsibility for all data owned by the NSW public health system is delegated by the Director-General to the Director of the Information Management and Clinical Systems Branch who acts, ex officio, as Data Administrator. The responsibilities of the Data Administrator are to:

- develop system-wide policies and procedures for the protection of data privacy
- define system-wide data access and custody arrangements

- ensure that compliance with data privacy policies and procedures is audited
- report to the Information Steering Committee (see 11.3.2).

11.3.2 Information Steering Committee

The role of the Information Steering Committee is to co-ordinate information management and technology policy and strategy development, which includes promoting information privacy principles and ethical information management practices.

11.3.3 Statewide Health Confidentiality and Ethics Committee (SHCEC)

The SHCEC is constituted in accordance with NHMRC guidelines for the protection of privacy in the conduct of medical research. This ethics committee undertakes assessment of requests for access to personal information held in data collections maintained at central administration. The SHCEC also considers:

- proposals for data use or issues requiring ethical advice referred by Department officers
- multi-centre research proposals
- proposals referred by RECs, and
- proposals for data linking.

See Appendix 4 for Terms of Reference.

11.3.4 Register of data collections

Each area health service or public health organisation which owns and administers one or more data collections should keep a register of these data collections. The Department should maintain a separate register of centrally administered collections. Each entry in the register should include:

- name of the data collection
- purpose or objective
- a summary statement of data items collected
- the Act or regulation which authorises the collection
- title of data sponsor
- title and contact point for data custodian
- statement of whether the collection includes personal health information.

11.3.5 Data sponsor

Every data collection identified in the register of data collections should have a nominated data sponsor who undertakes the duties of

ownership on behalf of the public health organisation, including:

- defining the purpose or objective of the data collection;
- establishing the scope and coverage of the collection;
- defining access and custody arrangements.

11.3.6 Data custodian

Every data collection identified in a register of data collections should have a nominated data custodian with responsibility for:

- ensuring a secure physical environment for data including backups and other safeguards, to prevent unauthorised access, destruction, use, modification or disclosure of data
- maintaining documentation, through the register, of the existence, content and format of the data collection
- maintaining a list of authorised data users
- authorising new data users and providing advice and assistance on any constraints which apply to use of the data
- determining and implementing appropriate levels of protection for the data
- dealing with requests for access to data other than from authorised data users, and ensuring that they are dealt with in accordance with relevant policies and procedures.

11.4 Access

11.4.1 Internal requests

11.4.1.1 Consistent with original purpose

Data custodians may approve use, within the public health system, of personal health information for purposes consistent with those for which it was collected, provided they are satisfied that:

- there is compliance with any constraints placed on the data
- use of the data is necessary for public health reasons or for the efficient and effective management of the health system
- the data will only be used for the project or purpose for which they have been requested
- adequate security exists to protect the data during transfer, and
- the data released and the number of people having access to the data are the minimum necessary to achieve the objectives of the project.

11.4.1.2 Not consistent with original purpose

Proposals to use data for a purpose not consistent with the original purpose of the data collection (such as linking or follow-up of individual subjects where consent has not been obtained) must be assessed by the Statewide Health Confidentiality and Ethics Committee (see 11.3.3) or a local REC, whichever is appropriate, who will make a recommendation regarding approval to the data custodian. The NHMRC Guidelines for the protection of privacy in the conduct of medical research[9] should be used in assessing proposals.

11.4.2 External requests

11.4.2.1 Approval

Requests from external applicants engaged in bona fide research or projects requiring data and wanting access to personal information should comply with the NHMRC Guidelines for the protection of privacy in the conduct of medical research[9], which specify that a properly constituted REC must consider every project which may breach one of the Information Privacy Principles (see Appendix 1). For the project to be approved, the REC must consider that its public benefit outweighs to a substantial degree the public interest in observing the IPPs.

11.4.2.2 Assessment of requests

Local RECs or the SHCEC should assess all external requests for access. Requests should be in writing and should contain:

- objective/purpose of the project
- exactly what data are required
- justification for using identifiable information
- methods of collection, use and protection of the data
- copies of research protocol or project proposal, consent forms, questionnaires etc.

The following criteria will be used to assess the request:

- are there any legal or other binding constraints on use of the data?
- is it essential that identifiable data be used for the project?
- is the requested level of access to data the minimum required for the success of the project?
- how significant is the research/project subject?
- is the research design or project proposal valid?

- does the applicant have the skills to successfully complete the project?
- does the public interest outweigh the right of the data subjects to privacy?
- what disposal procedures will apply?
- what security measures will apply?
- will informed consent be obtained from the subjects?
- if informed consent will not be obtained, what justification is there for this?

Based on the evaluation report of the REC or the SHCEC the Data Administrator (see 11.3.1) or appropriate Data Custodian (see 11.3.6) will approve or reject the request and advise applicants in writing of the Committee's recommendation, including reasons for denial of access and any conditions or restraints applying.

11.4.2.3 Conditions of access

If access is granted the principal applicant must sign an agreement to apply, as a minimum, the standards of privacy protection contained in this Code of Practice, and to abide by any other conditions or constraints (relating to charges, monitoring requirements etc.) on the use of the data set by the Data Administrator or Data Custodian.

Although NSW Health will endeavour to facilitate access to data by bona fide applicants, access is not guaranteed. Each request will be judged, and access granted or denied, on its own merits. The information supplied will always be the minimum required to meet a project's objectives.

Access, when granted, will be subject to the terms and conditions set out in an agreement, to be drawn up by the Data Administrator or Data Custodian and signed by the principal applicant. If access is refused, the reasons for refusal will be documented in a written response from the Data Administrator or Data Custodian. The applicant may choose to amend the proposal in the light of this response and re-submit it, in which case the assessment process will need to be repeated.

See Appendix 5 for flow charts illustrating lines of decision for approval of access to data.

11.5 Record linkage

11.5.1 Internal record linkage

11.5.1.1 Consistent with original purpose

Proposals for the linking of data obtained from different sources within the public health system may be approved by Chief Executive Officers, provided that:

- the purpose of the proposed linking is consistent with the original purpose for which the data were collected;
- use of the data is necessary for public health reasons or for the efficient and effective management of the health system; and
- the data will only be used for the purpose/project for which they were requested.

11.5.1.2 Not consistent with original purpose

Where the purpose of the proposed linking is not consistent with the original purpose for which the data were collected, the request must be referred to the SHCEC or an REC, whichever is appropriate, who will make a recommendation for approval or denial to the Data Administrator or Chief Executive Officer.

Proposals for data linking should include similar information as external requests for access to data (see 11.4.2). Criteria used in assessing proposals for data linking are similar to those used in assessing proposals for new data collections (see 11.6.2). Linking may be approved where:

- it is not proscribed by conditions under which the data were originally provided
- the objectives of the proposed project cannot be met efficiently or effectively in any other way.

If name, address, telephone number, Medicare number or other personal identifier obtained from an external source is to be used to effect linking, the Committee must be satisfied that no other mechanism (such as encrypted identification) is practicably available which could achieve the purpose of the research.

11.5.2 External record linkage

Requests to link data from a public health system data collection with

data from an external collection must be referred to the Statewide Health Confidentiality and Ethics Committee or a local REC who will make a recommendation for approval or denial to the Data Administrator or the Chief Executive Officer. Local RECs should inform the SHCEC of decisions made regarding all such requests received. Procedures are as for external requests for access to data (see 11.4.2).

11.6 Establishment of new data collections

11.6.1 Approval

All submissions for proposed new data collection projects or major revisions to existing collections which include identifiable or potentially identifiable information should demonstrate that the proposed collection conforms to this Code of Practice. Delegation to approve the establishment of new collections is as follows:

- statewide collections: the Data Administrator on advice of the Information Steering Committee
- collections spanning more than one area health service: the Data Administrator on advice of the Information Steering Committee
- organisation-based collections: the CEO.

The submission for approval should specify:

- purpose/objectives of the collection
- source and scope of data including list of data items
- data collection and storage methods
- procedures for dealing with requests for data to be used in other, unrelated projects
- guidelines for disclosure
- monitoring procedures to ensure compliance with these guidelines.

If informed consent will not be obtained from data subjects, reasons and justification should be given.

11.6.2 Assessment of submissions

In evaluating submissions for new data collections, the following criteria should be applied:

- do the data support the stated purpose of the data collection?
- can the data requirements be met in any other way (such as from an existing data collection)?

- to what extent will the collection contribute to
  - identification, prevention or treatment of disease; or
  - scientific understanding of health issues; or
  - improved service delivery?
- is the scope and coverage of the collection strictly limited to data required to achieve the stated objective and is the data of direct relevance to that objective?
- are the data items or collection procedures intrusive, or is there other risk of harm or embarrassment to the data subjects?
- are the data item definitions consistent with National health data dictionary[17] definitions?
- will informed consent be obtained?

11.7 Protection of data owned by external agencies

In regard to data owned by other agencies and being used by the Department, the provisions of this Code of Practice will be the minimum standard of protection afforded to these data. Furthermore, the Department will comply with any other legislation, protocols, codes of practice or guidelines relating to that data imposed by the owner of the data or another authoritative source considered appropriate by the Data Administrator.

11.8 Corporate network

The public health system corporate network is a telecommunications network which has the potential to link the Department, public health organisations and authorised external users and provide system-wide applications and functionality in a secure environment. It is not a central data base and does not store information.

11.8.1 Connections

All external connections to the corporate network should be approved by the organisation IT Director or appropriate Chief Executive Officer or General Manager. A record should be kept of all external connections.

11.8.2 Access

The same principles of information privacy, as expounded in this Code of Practice, should be applied to information accessed via the corporate network. Data may not be accessed, even if it is not downloaded, unless the purpose of the access is consistent with the

purpose for which the data were collected.

11.8.2.1 Downloading or other electronic transfer

Authorisation for downloading or other electronic transfer of data should not be given unless:

- the stated purpose of transfer or downloading is consistent with the purpose for which the data were collected, and
- the stated purpose has benefits substantial enough to justify such a use of the data.

Unless it is essential to achieve the stated purpose, identifying information such as name and address should be stripped or encrypted before transfer or downloading.

Local copies of data normally should be destroyed on completion of the task for which they were given. In some cases however it is necessary to archive data used for a particular project. If the data are to be retained for continued use rather than for archival purposes, they constitute a data collection and procedures for establishing a new data collection should be observed (see 11.6).

Refer to 9.1.4 for Internet transmission.

11.8.2.2 Security

Security will be provided in the corporate network through the use of:

- centralised and managed dial-in access
- secure gateway hardware and software to manage access from other networks such as the Internet
- filtering hardware to prevent undesirable and unnecessary traffic.

12 SECURITY

All stored personal health information, whether in hard copy, mainframe, laptop, home-based PC or any other medium, should be protected from unauthorised access, alteration or loss through the use of appropriate security devices and functions.

12.1 Mail and courier items

Packaging of mail and courier items should be secure and care should be taken that addresses are complete and correct.

12.2 Lists of codes

Master lists of codes assigned to clients/patients and details of coding systems should be stored separately from data to which they refer. Paper records which include master lists of codes assigned to individuals should be stored under lock and key.

Unauthorised access to master lists of codes stored in computer systems should be prevented by use of passwords and/or read-access protection of files.

Lists of codes should be sent via a different medium of communication from data to which they refer. For example, it is not sufficient to send the information and codes in two separate E-mail messages. A different medium such as courier delivery should be used.

12.3 Computer systems and applications

A secure physical and electronic environment should be maintained for all data held on computer systems. The Director-General may, in addition to the provisions set out in this Code of Practice, specify a minimum standard of physical and logical security for information held on computer systems.

12.3.1 Local procedures

CEOs should ensure that appropriate security procedures are developed for all computer systems and applications locally owned, operated or maintained.

Development of security procedures should be informed by Australian Standard 4444 Information Security Management[18] and by the Office

of Public Management's Security of information systems[19], which is based on the OECD information security principles.

12.3.2 Access control

Access should be restricted to a minimum number of authorised users. Each user's access should be limited to a necessary minimum and pre-agreed level.

12.3.3 Disposal of records

Disposal of data records should be done in such as way as to render them unreadable and leave them in a form from which they cannot be reconstructed in whole or in part.

12.4 Paper records

Paper source documents such as questionnaires and computer printouts should be generated and maintained so that names, addresses and other identifying data are not juxtaposed with medical or other personal information unless encrypted or otherwise rendered unintelligible.

12.4.1 Storage

All paper records should be kept in lockable storage when not in use. Basic precautions such as not storing records containing personal health information in a public area should not be overlooked.

12.4.2 Disposal

Paper records containing personal health information should be disposed of by shredding or burning. Where large volumes of paper are involved, specialised services for the safe disposal of confidential material should be employed. See 10.5.3 for disposal of health records.

13 PERSONNEL

13.1 Responsibility

Public health organisations should ensure that all employees are familiar with this Code of Practice and other appropriate guidelines, which includes having access to appropriate training. Each organisation should designate a specific officer to whom all requests for guidance on information privacy should be referred and who should ensure, as far as possible, that policies and procedures are observed.

13.2 Awareness

Policies and procedures are of little value if not routinely observed in practice at the service level. Ultimately, if a high level of information privacy is to be maintained, a personal commitment is required from health care workers. A culture of information privacy awareness needs to be fostered in the public health system.

It is essential that health care workers be made aware of their individual rights and responsibilities in respect of safeguarding information privacy. Health care providers in particular need to be informed about client/patients' rights of privacy and access. The importance of basic observances such as not discussing clients/patients publicly in a manner that would allow identification of individuals or groups, and keeping passwords secure, cannot be over-emphasised.

13.3 Staff training

Staff awareness of privacy issues should be promoted in a routine and ongoing way. Methods of doing this will vary, depending on the type of information and other characteristics of the local environment.

All staff should have training in privacy principles and requirements, with regular refresher courses. It is the responsibility of public health organisations to undertake such training. A privacy training kit is available to assist this process.

Notices reminding staff of the need to maintain confidentiality,
prominently displayed in appropriate places, are another way of promoting privacy awareness.

13.4 Staff agreement

Staff should be adequately informed of the existence of this Code of Practice and any other relevant rules and procedures, notably section 22 of the *Health Administration Act*, and have ready access to them. Staff should be required to sign an agreement not to access personal or other confidential information for their own purposes nor to disclose such information to an unauthorised person at any time, or to any other person except as permitted by this Code of Practice or other relevant policies and procedures. Prototype wording for an agreement may be found at Appendix 6; however alternative wording appropriate to local circumstances may be substituted.

These requirements apply to all public health organisations and personnel described in section 3.1. Systems programmers, maintenance and other technical personnel who have access to data bases from time to time are subject to the same requirements as regular data users.

The terms of the standard contract of employment should make it clear that breach of this undertaking will result in disciplinary action which may involve a fine or dismissal. The confidentiality undertaking shall remain in effect even after the staff member ceases to be employed in the public health system. In any case, section 22 of the *Health Administration Act* would still apply.

13.5 Contracted agencies

A responsible representative of every company contracted for data entry or other work which necessitates accessing identifiable information should sign a confidentiality agreement and be given a copy of this Code of Practice. The agreement should clearly set out responsibility for data security in transit and requirements for secure storage.

Detailed records of source documents sent off the premises for data entry, coding etc. should be kept and thorough checks made when returned to ensure that all records are returned.

14 IMPLEMENTATION AND REVIEW

14.1 Compliance

The implementation of this Code of Practice and any locally developed guidelines or rules, including dissemination and ensuring user compliance, is the responsibility of the relevant Chief Executive Officer. Appropriate penalties and disciplinary measures for breaches of the Code should be defined and enforced.

14.2 Public availability

This Code of Practice is a public document and may be viewed by members of the public who wish to be informed on how information privacy is protected within the NSW public health system. A copy should be kept at all health care facilities, libraries, area health service offices and at the Department of Health for this purpose.

14.3 Complaints

Complaints about breaches of client/patient privacy may be referred to the Health Care Complaints Commission. However, in the first instance, it is preferable for a client/patient to make his/her complaint direct to the Chief Executive Officer of the organisation where the problem occurred. Chief Executive Officers can also help to resolve complaints about privacy matters in their organisations. For the management of complaints regarding breaches of confidentiality of HIV/AIDS clients/patients, refer to Section 17 of the *Public Health Act*.

14.4 Review

This Code of Practice will be regularly reviewed to ensure continuing relevance and coverage of newly developing areas. Audit Branch, in conjunction with the Information Steering Committee, will develop an appropriate review protocol. Local policies and procedures should also be regularly reviewed and updated.

Referenced documents

1. Personal privacy protection in healthcare information systems (Australian Standard 4400). Standards Australia, 1996.

2. NSW Public service personnel handbook (loose leaf document, regularly updated).

3. Principles and minimum standards for the development of health services codes of conduct (NSW Health Circular 98/79).

4. Purchasing and supply manual. NSW Department of Health (loose leaf document, regularly updated).

5. Patient matters manual. NSW Health Department (loose leaf document, regularly updated).

6. Interagency guidelines for responding to adult victims of sexual assault. NSW Police Service, NSW Health Department, Office of Director of Public Prosecutions, 1995.

7. Subpoenas. (NSW Health Circular 98/29).

8. Ombudsman matters. (NSW Health Circular 91/91).

9. Aspects of privacy in medical research: an information paper and guidelines for the protection of privacy in the conduct of medical research. Canberra, National Health and Medical Research Council, 1995.

10. NSW Aboriginal health information Memorandum of Understanding. AHRC and NSW Department of Health, 1998.

11. Ethical code governing the provision of genetics services. NSW Department of Health, June 1998, (SWS) 98-0068, ISBN 0 7313 4036 1.

12. Guidelines for the use of genetic registers in medical research. Canberra, NHMRC, 1991.

13. Guidelines for data communication. Canberra, NPAAC, 1998.

14. Standard procedures for the use of health care interpreters (NSW Health Circular 94/10).

15. Health records and information manual for community health facilities. (loose leaf document, regularly updated). NSW Health Department, October 1991, HP no. (AB) 91/116, ISBN 0 7305 3525 8.

16. Register of health data collections, 3rd. ed. NSW Health Department, 1994. (IC) 94-05, ISBN 0 7310 0548 1.

17. National Health Data Dictionary. Canberra, Australian Institute of Health and Welfare, HWI 9, 1997.

18. Standard for information security management (Australian Standard 4444). Standards Australia, 1996.

19. Security of information systems. Office of Public Management, NSW Premier's Department, 1994. ISBN 0 7310 3642 5.

Appendix 1

Information Privacy Principles

Principle 1
Manner and purpose of collection of information
1. Personal information must not be collected by a collector for inclusion in a record or in a generally available publication unless:

a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information must not be collected by a collector by unlawful or unfair means.

Principle 2
Solicitation of information from individual concerned
1. Personal information is, where practicable, to be solicited directly from the individual concerned except where the individual authorises otherwise, or where information may be disclosed to the collector in accordance with these principles.
2. If:

a) a collector collects personal information for inclusion in a record or in a generally available publication; and
b) the information is solicited by the collector from the individual concerned,
the collector must take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual is informed of:
c) the purpose for which the information is being collected; and
d) if the collection of the information is authorised or required by or under law-the fact that the collection of the information is so authorised or required; and
e) the mandatory or voluntary nature of the information collection and the effects on the individual concerned (if any) of not providing all or any part of the requested information; and
f) the existence of the right of access to and rectification of the data relating to the individual; and
g) the name and address of the record keeper; and
h) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

Principle 3
Solicitation of information generally
If:

a) a collector collects personal information for inclusion in a record or in a generally available publication; and
b) the information is solicited by the collector,
the collector must take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:
c) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete; and
d) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual concerned.

Principle 4
Storage and information
A record keeper who has possession or control of a record that contains personal information must ensure that the information is:

a) stored for specified, explicit and lawful purposes and used in a way consistent with those purposes; and
b) adequate, relevant and not excessive in relation to the purposes for which it is stored; and
c) processed fairly and lawfully; and
d) kept for no longer than is necessary for the purposes for which the information is stored; and
e) protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
f) if it is necessary for the information to be given to a person in connection with the provision of a service to the record keeper, everything reasonably within the power of the record keeper is done to prevent unauthorised use or disclosure of the information.

Principle 5
Information relating to records kept by record keeper
1. A record keeper who has possession or control of records that contain personal information must, subject to clause 2 of this principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

a) whether the record keeper has possession or control of any records that contain any such information; and
b) whether the record keeper has possession or control of such a record relating to that person; and
c) if the record keeper has possession or control of any record that contains such information:
    i) the nature of that information; and
    ii) the main purposes for which the information is used; and
    iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record keeper is not required under clause 1 of this principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of this state that provides for access by persons to documents.
3. A record keeper must maintain a record setting out:

a) the nature of the records of information about individuals kept by or on behalf of the record keeper; and
b) the sources of information contained in those records; and
c) the purpose for which the information was collected and the authority for that collection; and
d) the purpose for which each type of record is kept; and
e) the classes of individuals about whom records are kept; and
f) the period for which each type of record is kept; and
g) the persons who are entitled to have access to information about individuals contained in the records and the conditions under which they are entitled to have that access; and
h) the steps that should be taken by persons wishing to obtain access to that information.

4. A record keeper must make the record maintained under clause 3 of this principle available for inspection by members of the public.

Principle 6
Access to records containing information about individuals
If a record keeper has possession or control of a record that contains personal information, the individual concerned is, without excessive delay or expense, entitled to have access to that record, except to the extent that the record keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of this state that provides for access by persons to documents.

Principle 7
Alteration of records containing information about individuals
1. A record keeper who has possession or control of a record that contains personal information must take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

a) is accurate; and

b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. If personal information has been corrected, deleted or added to in accordance with clause 1 of this principle, the individual concerned is entitled to have recipients of that information notified of the alterations by the record keeper.
3. The obligation imposed on a record keeper by clause 1 of this principle is subject to any applicable limitation in a law of this state that provides a right to require the correction or amendment of documents.
4. If:

a) the record keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of this state,

the record keeper must, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8
Record keeper to check accuracy etc. of personal information before use
A record keeper who has possession or control of a record that contains personal information must not use the information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date and complete.

Principle 9
Limits on use of personal information
A record keeper who has possession or control of a record that contains personal information must not use the information for a purpose other than for which it was collected and which was specified in accordance with principle 5 unless:

a) the individual concerned has consented to use of the information for that other purpose; or

b) the record keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person; or

c) use of the information is reasonably necessary for the enforcement (including investigations and the gathering of criminal intelligence) of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

d) use of the information for that other purpose is required or authorised by or under law; or
e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

Principle 10
Limits on disclosure of personal information
1. A record keeper who has possession or control of a record that contains personal information must not disclose the information to a person, body or agency (other than the individual concerned) unless:
a) the individual concerned has been informed under principle 2 that information of that kind is usually passed to that person, body or agency; or
b) the individual concerned has consented to the disclosure; or
c) the record keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person; or
d) the disclosure is required or authorised by or under law; or
e) the disclosure is reasonably necessary for the enforcement (including investigations and the gathering of criminal intelligence) of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public re venue, the record keeper must include in the record containing that information a note of that use.

Principle 11
Limits on use of certain information
1. Despite principles 9 and 10, information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life must not be used or disclosed by a record keeper without the express written consent, freely given, of the individual concerned, except to the extent that the record keeper is required or authorised to do so under the law of this state.
2. Information relating to an individual's criminal history may only be processed as required or authorised by law or a data protection code.

Appendix 2

Sample privacy warning for fax cover sheet

The information contained in this fax message is intended for the named addressee only. If you are not the intended recipient you must not copy, distribute, take any action reliant on, or disclose any details of the information in this fax to any other person or organisation. If you have received this fax in error please notify us immediately.

Appendix 3

Sample statement informing clients/patients about how their information may be used

The privacy and confidentiality of the information held about you will be respected. Confidential information about your health will only be given to another person if this is important for your care or is required or authorised by law.

Health care providers who are treating you, including those employed under contract such as Visiting Medical Officers, will have access to your health record regardless of where the treatment takes place. A discharge summary may be sent to your GP when you leave hospital.

Particular care will be taken to ensure strict control of access to certain sensitive records such as sexual assault, drug and alcohol, HIV/AIDS, domestic violence, sexual health, mental health, IVF and artificial insemination programs and records of children considered to be at risk. As a matter of principle, such records should not be accessed by health care providers in other areas.

On occasions information from health records may also be used for purposes such as teaching or research. Where possible your consent to such use will be obtained. Any person who has access to personal health information is bound by a duty of confidentiality.

You are entitled to see information about you held in your health record.

Under some Acts including the *Health Administration Act* and the *Public Health Act*, the Department of Health is required to collect certain information on clients/patients receiving treatment in the public health system. Some information about you is recorded in a computerised system, from which information is extracted and reported to the NSW Department of Health's head office. In nearly all cases names are removed before this information is reported. If it is proposed to link information about you from different sources you will have a chance to opt out.

Other authorities are legally entitled to certain information about matters such as Medicare eligibility, the registering of births and deaths, circumstances of death, drink-driving and cancer cases.

NSW Health has a comprehensive Code of Practice which sets out in detail arrangements for authorised access as well as requirements for safeguarding the privacy of your health information. Please ask to see a copy if you require more information.

Appendix 4

STATEWIDE HEALTH CONFIDENTIALITY AND ETHICS COMMITTEE (SHCEC)
Terms of reference

1 Overall objective

The NSW Health Department's Confidentiality and Ethics Committee has responsibility for providing ethical assessment of proposals to use departmental data collections for research or other purposes, of research proposals involving the Department, and of research proposals referred for consideration by other ethics committees.

In determining whether or not these proposals are ethically acceptable, the Committee examines the extent of their compliance with departmental policy on confidentiality and privacy, including the Information Privacy Code of Practice and standards for research ethics set down by the NHMRC.

2 Specific objectives

2.1 The Committee will assess proposals to use identifying or potentially identifying data held by the NSW Department of Health for research or other purposes; determine whether or not these proposals are ethically acceptable, and advise proponents and/or the Director-General accordingly. The requests to use data may seek to link datasets. They may emanate either internally (ie from within the NSW Department of Health) or externally.

2.2 The Committee's assessment of proposals will be in accordance with NHMRC guidelines pertaining to Research Ethics Committees. The Committee will function as a properly constituted ethics committee in accordance with those guidelines, and will report to the Australian Health Ethics Committee of the NHMRC on its compliance with the guidelines.

2.3 The Committee will provide assistance or advice to other ethics committees as required.

2.4 The Committee will consider multi-centre research studies or requests for data submitted by proponents or referred by other ethics committees.

2.5 The Committee will consider other research proposals or issues referred to it by Department of Health officers.

3 Membership

3.1 Composition

The Committee will have a minimum of seven members. The core membership will be in accordance with NHMRC guidelines and any amendments to them as issued from time to time. Currently these core categories are as follows:

- laywoman not associated with the institution
- layman not associated with the institution
- minister of religion
- lawyer
- medical graduate with research experience.

In addition the membership will include a nominee of the Deputy Director-General, Public Health and Chief Health Officer, and a nominee of the Director, Information Management and Clinical Systems, NSW Department of Health. The Chief Health Officer's nominee may concurrently fulfil one of the core NHMRC categories.

3.2 Appointment
Members of the Committee are appointed by the Director-General of the NSW Health Department.

3.3 Tenure
Members are appointed for a term of two years and may serve consecutive terms.

3.4 Chairperson
The Chairperson will be appointed by the Director-General of the NSW Department of Health.

3.5 Secretary
Secretariat services will be provided or arranged by the Department. The Secretary may participate in every aspect of the Committee's deliberations, but cannot be considered as representing one of the essential categories of membership for the purposes of decision making.

4 Reporting
4.1 Line of responsibility
The Committee is responsible to the Director-General, NSW Department of Health. The Committee will furnish annual reports to the Director-General on its activity and its compliance with the reporting and monitoring requirements of the NHMRC.

The Committee will also provide reports to the Australian Health Ethics Committee of the NHMRC in accordance with the requirements of the NHMRC.

4.2 Reports on ethical assessments
With the concurrence of members, the Chair of the Committee will report in writing to the principal proponent on the Committee's determination of the ethical acceptability of individual proposals.

Where a proposal is referred to the Committee by another Ethics Committee, the Chair of the Committee will report in writing on the Committee's deliberations to the Chair of that committee. In this circumstance the Chair of the Committee will not correspond directly with the proponent.

5 Mode of operation
5.1 Meeting frequency
The Committee will meet on a regular basis as determined by the demand for ethical assessments. In general the Committee will meet at least four times a year.

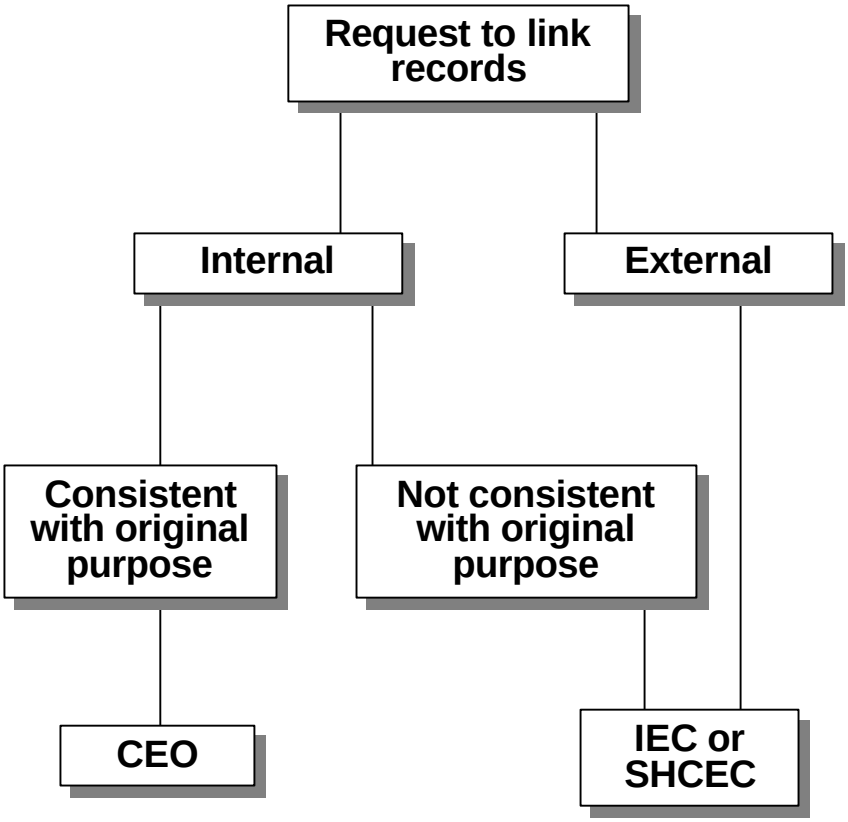
5.2 Quorum
A quorum comprises a minimum of five members in attendance at a meeting. At least two of these members must be external to the Department and at least two must not be medically or scientifically trained. However in the event of of one or more representatives of compulsory categories of membership not being in attendance at a meeting, an ethical determination cannot be made without oral or written comment from the absent representative/s.

Where a unanimous decision concerning the ethical acceptability of a proposal is not reached, the decision will be considered to be carried by a majority of two-thirds of members who examined the proposal, provided that the majority includes at least one layperson.

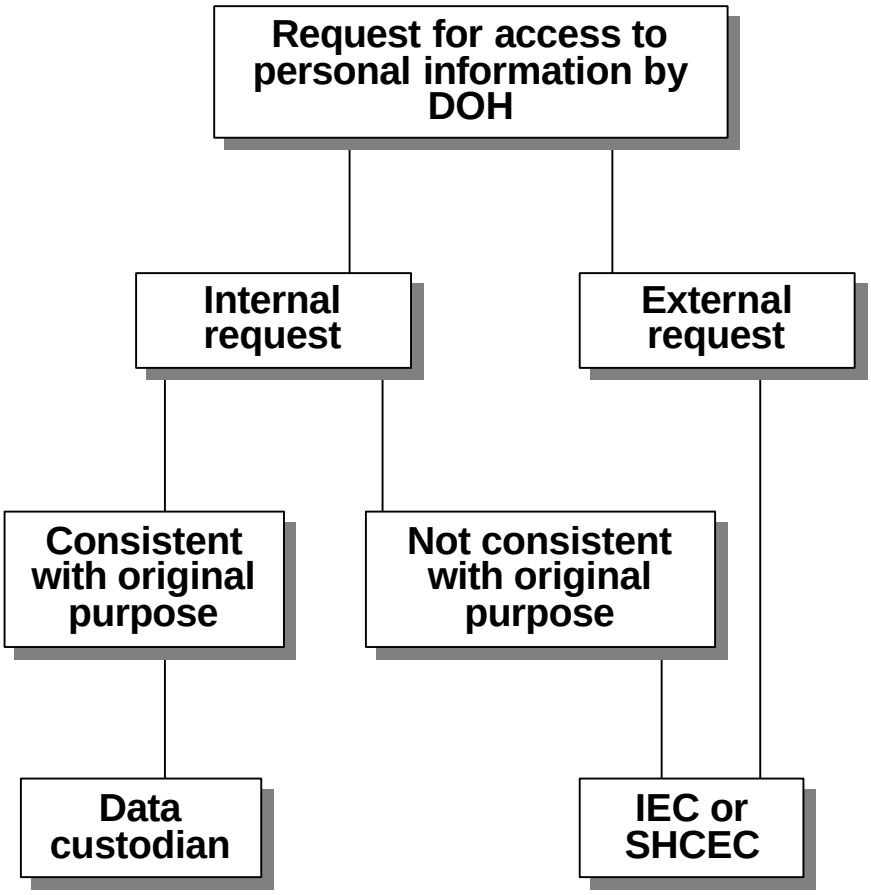
Attendance at a meeting may be in person or via a telecommunications link.

APPENDIX 5

Decision path for requests to link records from two or more



APPENDIX 5


Request for access to personal information by DOH
Internal request
External request
Consistent with original purpose
Not consistent with original purpose
Data custodian
IEC or SHCEC

Appendix 6

Sample undertaking to observe privacy requirements

I, (name).....understand that, while I am employed by the NSW Department of Health, I may have access to confidential data or information collected for purposes of client/patient care or for administrative, statistical or other purposes. Such confidential information includes the identity of, and personal and health information about individual persons.

I undertake not to knowingly access any personal health information unless such information is essential for me to properly and efficiently perform my duties. I undertake strictly to preserve the confidentiality of this information and I understand that a breach of this undertaking will result in disciplinary action. I acknowledge my statutory duty under Section 22 of the *Health Administration Act 1982* (attached), in relation to the disclosure of information. In order to fulfil this undertaking, I will not divulge any identifying, personal or health information regarding individual persons, except to authorised staff of the NSW Department of Health who require such information to carry out the functions of the Department.

I also undertake to follow other information privacy and security procedures as stipulated by the Director-General, in relation to any personal health information which I access in the course of my duties. In order to fulfil this undertaking I will ensure that, so far as is within my control, such information, whether in the form of paper documents, computerised data or in any other form, cannot be viewed by unauthorised persons, and that the information is stored in a secure and orderly manner which prevents unauthorised access.

I further undertake to inform my supervisor immediately if I become aware of any breach of privacy or security relating to the information which I access in the course of my duties.

Signed.....in the presence of

(name).....

(signature).....

(position).....

Date.....

INDEX