Australian Government

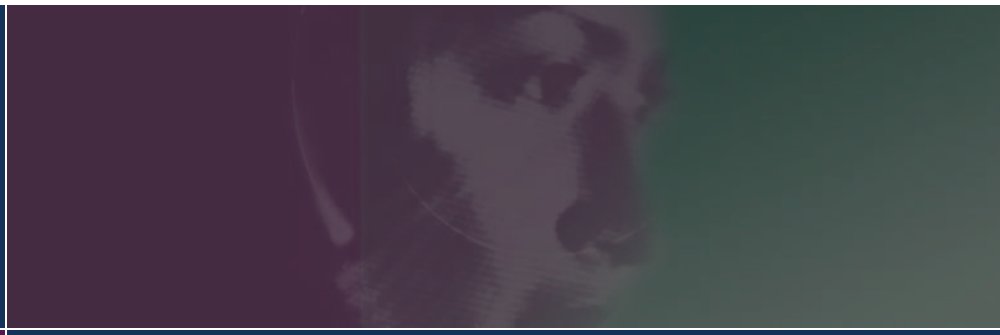
National Health and Medical Research Council

The Regulation of Health Information Privacy in Australia

A description and comment

Prepared by Professor Colin Thomson

JANUARY 2004



INVESTING IN AUSTRALIA'S HEALTH

Australian Government

National Health and Medical Research Council

National Health and Medical Research Council Privacy Committee

The Regulation of Health Information Privacy in Australia

A description and comment

Professor Colin Thomson

January 2004

Paper-based publications

© Commonwealth of Australia 2004

Electronic documents

ISBN Print: 1864962941 Online: 1864962887

To obtain details regarding NHMRC publications contact:

Email: nhmrc.publications@nhmrc.gov.au
Phone: Toll Free 1800 020 103 Extension 9520
Internet: http://www.nhmrc.gov.au

TABLE OF CONTENTS

Introduction v

Summary vii

PART ONE

Privacy Regulation in Australia

Overview 1

PART TWO

The Privacy Act 1988: Commonwealth and ACT 3

PART THREE

The Privacy Act 1988: Private Sector 11

PART FOUR

States/Territories with Private Sector Privacy Legislation

Australian Capital Territory 24

Victoria 28

New South Wales 35

PART FIVE

State/Territory Legislation/Regulation in the Public Sector

Australian Capital Territory 41

New South Wales 41

Northern Territory 45

Queensland 48

South Australia 53

Tasmania 54

Victoria 56

Western Australia 58

PART SIX

National Health Privacy Code 59

PART SEVEN

International

European Parliament and Council of Europe 67

United States of America 70

New Zealand 71

Canada 80

INTRODUCTION

In mid 2003 the NHMRC identified privacy as a priority issue that needed investigation. Specifically, NHMRC was being told that the privacy framework surrounding health information in Australia was restricting health and medical research and health care delivery. These messages were coming from researchers, health consumers, medical practitioners, data custodians and human research ethics committees.

Mindful of the intention to review the *Privacy Amendment (Private Sector) Act 2001* two years after its introduction, the NHMRC agreed that it would be timely to investigate these claims with a view to providing a detailed, reasoned and evidence-based submission to the review of the privacy legislation.

NHMRC established a working committee with three major tasks:

1. Undertake an analysis of the privacy framework in Australia, as it relates to health information.
2. Undertake consultation with NHMRC's stakeholders to document their attitudes towards and perceptions of the privacy framework as well as their experiences.
3. Prepare a submission to the review of the privacy legislation when the review is announced.

The first task above is the subject of this paper.

The NHMRC commissioned Professor Colin Thomson, NHMRC Consultant in Ethics, to:

1. Examine and document privacy regulation in Australia at the Commonwealth, as well as the State and Territory level. Regulation includes legislation, codes of practice and guidelines.
2. Identify and document elements of that regulation, on a state by state basis, that have potential to impinge upon the conduct of activities that NHMRC is committed to promote or for which NHMRC has responsibility namely:
   - Public health and medical research
   - Providing public health advice
   - Maintaining high ethical standards in research.
3. Examine privacy regulation in comparable overseas jurisdictions, including the European Union, with a view to identifying whether these issues have arisen overseas and, if so, whether any action has been taken to address them. Are alternative models available to address undesirable impacts?

The research for this paper took place during August and September 2003. The legislation and other documents cited were accessed at that time and, especially where these were in draft form, may have been superseded by the time of publication.

This paper does not purport to provide legal advice to the reader. It is intended only as a description of the various privacy provisions relevant to health information and, in places, includes analysis of or comment on those provisions.

SUMMARY

1. Privacy regulation refers to legislative or administrative schemes of regulating the handling of certain information about citizens by public and private agencies and organisations. "Information privacy" or "data protection" are expressions sometimes used to refer to such schemes.

2. Information privacy protection typically involves limits or conditions on the collection, storage, access, use and disclosure of personal, identifying information. Some regulatory schemes are general in that they apply to any such information: others are specific in that they apply only to some categories of such information, usually health information.

3. The underlying public policy issue that underlies these regulatory schemes is the balance between, on the one hand, the public interest in protecting individual privacy and, on the other, the public interests in using that information for the benefit of others.

4. In Australia, the regulatory schemes can be conveniently represented in the following table.

JURISDICTION	PUBLIC SECTOR	PRIVATE SECTOR - GENERALLY	PRIVATE SECTOR - HEALTH
Commonwealth	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
Australian Capital Territory	Privacy Act 1988 (Clth) Health Records (Privacy and Access) Act 1997	Privacy Act 1988 (Clth)	Health Records (Privacy and Access) Act 1997 Privacy Act 1988 (Clth)
New South Wales	Privacy and Personal information Protection Act 1998 Health Records and Information Privacy Act 2002 (in force 2004)	Privacy Act 1988 (Clth)	Health Records Information Privacy Act 2002 (in force 2004) Privacy Act 1988 (Clth)
Northern Territory	Information Act 2002	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
Queensland	Information Standards 42 (general) & 42A (health)	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
South Australia	Information Privacy Principles	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
Tasmania	Information Privacy Principles 1997	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
Victoria	Information Privacy Act 2000 Health Records Act 2001	Privacy Act 1988 (Clth)	Health Records Act 2001 Privacy Act 1988 (Clth)
Western Australia	Health Act 1911 section Criminal Code sections	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth) Confidentiality of Health Information Committee

* The table does not record the fact that all jurisdictions also use regulatory schemes, often legislative, to govern the use or disclosure of information gained by public employees in the course of their duties.

5. Public sector regulation of privacy in Australia is of three types:
   (a) confidentiality or secrecy provisions. All nine jurisdictions have such regulation that can apply generally, eg to all employees and all information or specifically, eg to some employees and to specific types or registers of information.
   (b) privacy legislation or regulation applying to all public agencies. The Commonwealth, the Australian Capital Territory, New South Wales, the Northern Territory and Victoria have legislation of this type. All other jurisdictions, except Western Australia, have relied on administrative guidelines. These would generally be treated as subject to other legislation, a status that is made explicit in Queensland.
   (c) health information privacy legislation that limits handling of health information. New South Wales and Victoria have such subject specific legislation, while Northern Territory includes such information specific controls in the general legislation.

6. These schemes limit agencies by requiring them to abide by a set of principles as to collection, storage, security, access, use and disclosure of personal or health information. Generally speaking, the principles prohibit use or disclosure of such information for purposes other than that for which the information was collected ('secondary purposes') unless there is consent, an emergency, a law enforcement justification or an administrative determination, either specific to the case or by a standing direction or exemption. The criteria for such directions or exemptions are not always made clear but, where it is, it is usually referred to as the public interest.

7. The Commonwealth, New South Wales and Victorian schemes provide for an external, situation specific, review stage in permitting use and disclosure of personal information for medical research (Clth) or health information for a variety of purposes (including research) (NSW and VIC) where consent, emergency or law enforcement justifications are not available. This stage relies on Human Research Ethics Committees (HREC) to consider specified matters and determine whether or not, in their opinion, the public interest in the proposed use, eg research, outweighs or does not outweigh the public interest in protecting privacy. However, even where an HREC does conclude that the public interest balance is in favour of the use or release, the public sector agency that holds the information may still decline to use or disclose it in the manner that the HREC has approved.

8. Private sector regulation of information privacy is of two types:
   (a) the Commonwealth Privacy Act limits some private sector organisations in relation to handling of any personal information and private sector health service providers in their collection, storage, access, use and disclosure of health information.
   (b) in NSW and Victoria, state legislation limits private sector health service organisations in collection, storage, access, use and disclosure of health information.

9. These schemes operate in a similar fashion to the public sector schemes by requiring organisations to conform to sets of principles about their collection, storage, access, use and disclosure of health information. They rely on human research ethics committees to review requests to collect, use or disclose health information for secondary purposes where the consent, emergency and law enforcement justifications are not available. As with the public sector schemes, even where an HREC has concluded that the balance of the public interests is in favour of use or disclosure, the private sector organisation may decline to do so.

10. The Council of Europe, the United States of America, Canada and New Zealand have regulated for the protection of privacy. The federal regimes vary in the level of detail, but those where there is a similar level of detail as in Australia appear to have adopted a standard that is less exacting. An example of the essence of the difference is in relation to use and disclosure for a secondary purpose. This is permitted, typically, on conditions that consent is impracticable, that the purpose cannot be achieved using non-identifying information and that the information will not be published in identifying form. Reliance on ethics committee review appears to be used in the United States, some Canadian provinces and in New Zealand. However, in the United States the ethics committee's task is to waive consent, in Canada it may be specific to the privacy issue but in New Zealand it appears to be no more than the usual ethical review of the research.

PART ONE

PRIVACY REGULATION IN AUSTRALIA

OVERVIEW

Privacy and Information Privacy

The concept of privacy can be related to several domains of an individual's life – their physical environment, the representation of their appearance as well as information about them. The legislation to which this analysis relates is confined to information privacy – the protection of the privacy of information about a person.

Constitutional considerations

The Australian Constitution does not expressly protect privacy nor does it contain an unambiguous head of Commonwealth legislative power on which to base legislative protection. The preamble to the Privacy Act 1988 (Privacy Act) attracts paragraph 51(1)(xxix) the "external affairs" head of legislative power and relies on Australia's being party to the International Covenant on Civil and Political Rights and to its membership of the Organisation for Economic Co-operation and Development as the requisite external affairs.

The constitutional basis of the Privacy Act, especially in its extension to the private sector has not been judicially challenged.

Section 109 of the Constitution provides that where there is an inconsistency between a law of the Commonwealth and a law of a State, the latter shall be void to the extent of that inconsistency. Judicial construction of this provision has concluded that the test of whether there is such an inconsistency depends on the expression of the intent of the Commonwealth Parliament when it passed the law in question. It is clear from section 3 of the Privacy Act 1988, that the parliament did not intend to affect the operation of laws of States and Territories relating to privacy that are capable of operating concurrently with the Privacy Act. It is also clear from the definition of "organisation" in section 6C of the Privacy Act, that it does not, with a few exceptions, purport to regulate the activities of State departments, agencies or bodies.

As a result of the expression of this intent, there are legislative and administrative provisions designed to protect privacy at Commonwealth, State and Territory levels. This leads to overlapping of regulatory schemes and to the subjection of some activity to both Federal and State regulation. This also presents some difficulties in providing this analysis in a way that is useful and not unduly confusing. The following table reflects the present situation:

JURISDICTION	PUBLIC SECTOR	PRIVATE SECTOR - GENERALLY	PRIVATE SECTOR - HEALTH
Commonwealth	Privacy Act 1988	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
Australian Capital Territory	Privacy Act 1988 (Clth) Health Records (Privacy and Access) Act 1997	Privacy Act 1988 (Clth)	Health Records (Privacy and Access) Act 1997 Privacy Act 1988 (Clth)
New South Wales	Privacy and Personal Information Protection Act 1998 Health Records and Information Privacy Act 2002 (in force 2004)	Privacy Act 1988 (Clth)	Health Records and Information Privacy Act 2002 (in force 2004) Privacy Act 1988 (Clth)
Northern Territory	Information Act 2002	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
Queensland	Information Standards 42 (general) & 42A (health)	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
South Australia	Information Privacy Principles Instruction 1992	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
Tasmania	Information Privacy Principles 1997	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth)
Victoria	Information Privacy Act 2000 Health Records Act 2001	Privacy Act 1988 (Clth)	Health Records Act 2001 Privacy Act 1988 (Clth)
Western Australia	Health Act 1911 section Criminal Code sections	Privacy Act 1988 (Clth)	Privacy Act 1988 (Clth) Confidentiality of Health Information Committee

From this it can be seen that the Privacy Act is central to protection of information in the activities of Federal agencies and of certain organisations in the private sector.

It will be convenient to describe and comment on the pattern of its regulation of the Federal public sector and then of the private sector, dealing in turn with complementary legislation in those States that have regulated any element of the private sector. Following that, separate descriptions and comments are provided about State regulation of State level public sector.

Finally, some comparative accounts are provided of legislation in the European Community, the United States of America, Canada and New Zealand.

PART TWO

THE PRIVACY ACT 1988 COMMONWEALTH AND AUSTRALIAN CAPITAL TERRITORY

PUBLIC SECTOR

By enacting the Privacy Act, the Commonwealth has regulated the protection of information privacy by requiring its public sector agencies to abide by the Information Privacy Principles (IPPs). Traditionally, before privacy became a regulatory subject, Commonwealth legislation contained general prohibitions directing public sector employees not to use or disclose information otherwise than in the course of their work. These provisions remain and some will be dealt with in relation to the conditions on disclosure in the IPPs.

Date of Commencement

The Privacy Act, so far as it regulates the Commonwealth public sector commenced on 1 January 1989 and so applied to all information collected from that date.

The important aspect of commencement dates is that the IPPs do not apply to information collected before 1 January 1989. This may release some agencies from the constraints of the IPPs dealing with use and disclosure.

Scope of application

Throughout this analysis, it will be repeatedly important to establish the precise scope of privacy legislation. This can usually be achieved by identifying the entities subject to the Privacy Act and the information as to which their activities are regulated.

Agencies

In the Commonwealth public sector, all agencies are subject to the IPPs. These are defined in section 6 in an exhaustive manner and, for present purposes, it will be assumed that all Commonwealth agencies are included.

Personal information

The information to which the IPP obligations apply is defined in section 6 as personal information that is contained in a record. Both elements are defined:

"**personal information** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

"**record means**:

(a) a document; or

(b) a database (however kept); or

(c) a photograph or other pictorial representation of a person;
but does not include:

(d) a generally available publication; or

(e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or

(f) Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act; or

(fa) records (as defined in the *Archives Act 1983)* in the custody of the Archives (as defined in that Act) in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or

(g) documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980;* or

(h) letters or other articles in the course of transmission by post."

It is in respect of personal information that is contained in a record that the IPP obligations are imposed.

Intrinsic identifiability?

One essential element of the definition of personal information is that the identity of the individual is apparent, or can reasonably be ascertained, *from the information or opinion*. An important issue is whether this means that coded information is personal information for the purposes of the Privacy Act. Arguably it is not because the identity of an individual cannot be reasonably ascertained from the information – it cannot be ascertained without using the code *in addition* to the information. Where coded sets of information are re-united with identifiers to create an identifying data set, the privacy principles will then apply to that data set.

Guidelines by the Federal Privacy Commissioner do not clarify this issue. The Guidelines on Privacy in the Private Health Sector, at p vii, state that:
"The NPPs do not apply to de-identified information or statistical data sets, which would not allow individuals to be identified".

By contrast, the *National Statement on Ethical Conduct in Research Involving Humans* (the National Statement) refers to "potentially identifiable" information, being typically coded information from which identifiers have been removed but can be replaced. Such information may not fall within the Privacy Act definition of "personal information" and, if so, would not be subject to statutory regulation. However, such information would be subject to the National Statement's standards because the National Statement does not treat such information as de-identified.

Potential impingement on NHMRC

(a) Agency functions

As a Commonwealth agency, NHMRC is bound by the IPPs. This means that in collection, access, use and disclosure of personal information for inclusion in or contained in a record, the NHMRC must meet the IPPs.

Grant Process

The NHMRC will collect personal information about grant applicants and, accordingly, it needs to ensure that

- information is necessary for or directly related to its (granting) purpose;
- individuals are notified of the matters in IPP 2, ie, purpose, authority and bodies to whom the information is usually disclosed;
- information is kept securely;
- it takes reasonable steps to provide access under IPP 5;
- it keeps a record of the nature of personal information it has;
- it grants access to that information;
- it keeps the information accurate;
- it uses the information only for relevant purposes and not for purposes other than that for which it was collected, (with some exceptions), and
- it does not disclose the information, (with some exceptions).

If the purpose of the collection of this information is to assess eligibility for research grants, then the NHMRC needs to ensure that it informs applicants to whom, if anyone, it will in usual practice disclose this for the purposes of assessment. This would require disclosure about assessment panels and careful assessment as to whether information about grant applicants can be used to investigate research fraud or misconduct, on the basis that this is a purpose authorised by law, directly related to the collection purpose or necessary for the protection of the public revenue. These would seem to be readily arguable.

(b) Activities that NHMRC promotes

This is likely to arise where researchers wish to gain access, for use in a project funded by the NHMRC, to personal information held by an agency. IPP 11 prevents an agency from so using the information unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(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;

(d) the disclosure is required or authorised by or under law; or

(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Some agencies are governed by their own legislation and this may permit disclosure under exception (d). For example, section 90 and 91AB of the *Commonwealth Electoral Act 1918* permit the Australian Electoral Commission to provide information from the electoral roll and section 29 of the *Australian Institute of Health and Welfare Act 1987* permits some disclosure of information held by officers of the Institute.

Section 95 of the Privacy Act

Section 95 of the Privacy Act allows an agency to do an act that would otherwise be a breach of an IPP where that act is done in the course of medical research and in accordance with guidelines issued by the NHMRC and approved by the Privacy Commissioner.

The section 95 guidelines authorise human research ethics committees (HRECs) to balance the public interest in the protection of privacy with the public interest in the proposed research. If they conclude that the latter outweighs the former to a substantial degree, they provide an agency with the basis for deciding to act, usually by disclosing personal information, in a way that would otherwise infringe an IPP or IPPs. However, an agency can, notwithstanding an HREC decision, decline to disclose the information.

This exception from the obligations of Federal agencies is available only for use or disclosure of personal information for medical research. This term is defined in the Privacy Act which states only that it "includes epidemiological research."

The research funded by NHMRC may include research that does not fall within that definition of medical research and to the extent that this is so, personal information for such research can only be disclosed by a Federal agency acting *within* the IPPs.

The justification for the confinement of the section 95 guidelines to medical research is not obvious, and has become less obvious since the introduction in 2001 of the National Privacy Principles (NPP) that employ the wider concept of research related to public health or public safety.

Other requirements of section 95 and the Section 95 Guidelines

The section 95 guidelines require the detailed provision of information by a researcher and its assessment by an HREC. The list of required information as set out in clause 2.4 is:

(a) the aims of the research;

(b) the credentials and technical competence of the researcher;

(c) the data needed and how it will be analysed;

(d) the source of the data;

(e) the study period;

(f) the target population;

(g) the reasons why identified* or potentially identifiable* information is needed rather than de-identified* information, and the reasons why it is not proposed to seek consent to the use of personal information. [Note: Any genetic research should be conducted in accordance with the principles in '16. Human Genetic Research' of the *National Statement on Ethical Conduct in Research Involving Humans* (1999) when considering the release of personal information, and genetic testing.]

(h) the specific uses to which the personal information used during the study will be applied;

(i) the proposed method of publication of results of the research;

(j) the estimated time of retention of the personal information;

(k) the identity of the custodian(s) of the personal information used during the research;

(l) security standards to be applied to the personal information. In particular, that personal information will be retained in accordance with the *Joint NHMRC/AVCC Statement and Guidelines on Researc* (Appendix 3), and in a form that is at least as secure as it was in the sources from which the personal information was obtained unless more stringent legislative or contractual provisions apply;

(m) a list of personnel with access to the personal information;

(n) the standards that will be applied to protect personal information disclosed by a Commonwealth agency. These should include the:

  (i) terms of any disclosure agreement between the agency and the researcher to govern the limits on use and disclosure of that personal information; and

  (ii) proposed methods of disposal of the personal information on the completion of the research, and that these are in accordance with the *Archives Act, 1983* for Commonwealth records and legislative requirements of a State or Territory; and

  (iii) standards that will be applied to protect privacy of personal information where it is made available to other researchers or third parties if that is proposed.

This information significantly exceeds the information that an HREC would normally require from a researcher for the purpose of reviewing and deciding on the ethical acceptability of a research proposal and to that extent it involves an imposition on researchers that they may regard as an impediment.

Further, when reviewing that information provided by a researcher, an HREC is required to consider whether it has sufficient information, expertise and understanding of privacy issues, either amongst the members of the HREC or otherwise available to it, to make a decision that takes proper account of privacy. Though plainly relevant to the Privacy Act, it is questionable whether these matters are within the scope of research ethics to which HRECs primary duties are directed.

Further, the consideration requires some skill in statutory interpretation for which the membership of HRECs was not designed.

Even if this is conceded, the guidelines then require an HREC to identify and consider the IPP or IPPs that might be breached in the course of the proposed research, including whether it is necessary for the research to use identified or potentially identifiable data, and whether it is reasonable for the research to proceed without the consent of the individuals to whom the information relates. Then, the HREC is to ensure that the committee has the competence to determine if the public interest in the proposed research outweighs, or does not outweigh, to a substantial degree, the public interest in the protection of privacy. If the public interest in the proposed research does not outweigh, to a substantial degree, the public interest in the protection of privacy then the research should not be carried out.

The matters that an HREC is required to consider in weighing the public interest are set out in clause 3.3:

(a) the degree to which the medical research is likely to contribute to:
- the identification, prevention or treatment of illness or disease; or
- scientific understanding relating to health; or
- the protection of the health of individuals and/or communities; or
- the improved delivery of health services; or
- scientific understanding or knowledge.

(b) any likely benefits to individuals, to the category of persons to which they belong, or the wider community that will arise from the medical research being undertaken in the manner proposed;

(c) whether the medical research design can be satisfied without risking infringement of an IPP and the scientific defects in the medical research that might arise if the medical research was not conducted in the manner proposed;

(d) the financial costs of not undertaking the medical research (to government, the public, the health care system, etc);

(e) the public importance of the medical research;

(f) the extent to which the data being sought are ordinarily available to the public from that Commonwealth agency; and

(i) whether the medical research involves use of the data in a way which is inconsistent with the purpose for which the data were made public; and

(ii) whether the medical research requires an alteration of the format of the data of a kind that would, if used by an agency, involve a breach of an IPP.

(g) whether the risk of harm to a person whose personal information is to be used in proposed research is minimal, having regard to the elements of that research provided in response to paragraph 2.3 of these guidelines;

(h) the standards of conduct that are to be observed in medical research, including:

(i) the study design and the scientific credentials of the researchers;

(ii) if the research involves contact with participants, the procedures or controls which will apply to ensure that participants are treated with integrity and sensitivity, including whether questions to be asked or procedures to be employed are intrusive;

(iii) whether access to personal information is restricted to appropriate researchers;

(iv) the risk that a person or group could be identified in the published results; and

(v) the procedures that are to be followed at the completion of the research to ensure that all data containing personal information are at least as secure as they were in the sources from which the data were obtained, including the date when the data will be destroyed or returned.

Even if this information is provided by the researcher, it is a daunting list of matters and when combined with the detailed requirement to record decisions contained in paragraph 3.4, can be a heavy additional workload for an HREC.

The Guidelines also impose on the Australian Health Ethics Committee (AHEC) the responsibility to report annually to the Privacy Commissioner "details of the research projects conducted under these guidelines and include evaluation of the operation of the guidelines for the year of reporting". (Guidelines paragraphs 5.1, 5.2).

However, these impingements on the operations of HRECs may not be as severe as is suggested. A study of the use of the s95 guidelines completed for the year 2000–2001 showed that the guidelines were relied on in reviewing a total of 42 proposals, a small proportion of the 15,050 proposals that HRECs in Australia reported reviewing that year.

PART THREE

THE PRIVACY ACT 1988

PRIVATE SECTOR

Since 21 December 2001, the Privacy Act has applied to certain organisations in the private sector in relation to the collection and handling after that date of personal information.

Scope

The scope of application to the private sector is determined by definitions of organisation, sensitive information and health information.

Organisations are defined to include virtually all individuals and corporations, but exclude (Federal) agencies, State and Territory authorities or instrumentalities and small business operators with an annual turnover of less than $3million. The resulting application to such large organisations in their handling of personal information is unlikely to have potential impact on the functions of NHMRC.

However, the definition of "small business operators", who are excluded from the application of the Act, does not apply to any individual, body corporate, partnership, unincorporated association or trust that provides a health service to another individual and holds any health information except in an employee record; or discloses personal information about another individual to anyone else for a benefit, service or advantage; or provides a benefit, service or advantage to collect personal information about another individual from anyone else; or is a contracted service provider for a Commonwealth contract (whether or not a party to the contract).

The definitions of sensitive information, health information and health service in section 6 are:

"**sensitive information** means:

(a) information or an opinion about an individual's:
  (i) racial or ethnic origin; or
  (ii) political opinions; or
  (iii) membership of a political association; or
  (iv) religious beliefs or affiliations; or
  (v) philosophical beliefs; or
  (vi) membership of a professional or trade association; or
  (vii) membership of a trade union; or
  (viii) sexual preferences or practices; or

(ix) criminal record; that is also personal information; or

(b) health information about an individual.

"health information means:

(a) information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individual's expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual; that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances".

"health service means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:

(i) to assess, record, maintain or improve the individual's health; or

(ii) to diagnose the individual's illness or disability; or

(iii) to treat the individual's illness or disability or suspected illness or disability; or

(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist".

"**contracted service provider, for a government contract,** means:

(a) an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to an agency or a State or Territory authority under the government contract; or

(b) a subcontractor for the government contract".

Potential Impingement on NHMRC

(a) Agency functions

The implications for NHMRC are that the Privacy Act and therefore the National Privacy Principles apply to its contractors and, secondly, that any research activity that involves a health service provider is also subject to the Act. The NHMRC has an interest in ensuring that contractors and health service providers who conduct research activities that it supports, comply with the Act.

The latter consequence means that any activity conducted by a health service provider, not merely medical research, that uses health information must be

conducted in conformity with the NPPs. Where NHMRC funds or promotes research, it will need to determine whether it is conducted by a health service provider, ie one who provides a health service (as defined) AND who has health information in order to decide what conditions need to be satisfied to ensure that the research is conducted lawfully.

The definition of health information leaves uncertain the question of whether it includes genetic information, which can be, but is not always, health information. In *Essentially Yours* (ALRC/NHMRC 2003) it was recommended that the Privacy Act be amended to make clear that genetic information is within the meaning of health information.

(b) Activities that the NHMRC promotes

These implications for NHMRC relate to the manner in which health information can be collected, used or disclosed for research and the limitations imposed on such collection, use or disclosure by the NPPs.

The relevant NPPs regulate the collection, storage, use and disclosure of health information, a sub-set of sensitive information which is in turn a sub-set of personal information. The following discussion addresses issues of collection and then issues of use and disclosure, following the sequence of NPP10.

Collection with consent

NPP 10.1 states the limits on the collection of sensitive information and NPP 10.2 and 10.3 relax those limits in relation to health information.

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit organisation – the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

"non-profit organisation" means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

The Act provides that "consent means express consent or implied consent" and the guidelines on Privacy in the Private Health Sector explain what this means:

Key elements of consent

The key elements to consent are:

- it must be provided voluntarily;
- the individual must be adequately informed; and
- the individual must have the capacity to understand, provide and communicate their consent.

Consent must be voluntary – the individual must have a genuine opportunity to provide or withhold consent; that is, they must be able to say 'yes' or 'no' without extreme pressure which would equate to an overpowering of will.

Consent must be informed – the individual must know what it is they are agreeing to. In other words, the individual needs to be aware of the implications of providing or withholding consent, having received the information in a way meaningful to them and appropriate in the circumstances.

The individual must have the capacity to provide consent – the individual must be capable of understanding the issues relating to the decision, forming a view based on reasoned judgment and communicating their decision.

Express or implied consent

The Privacy Act states that consent may be 'express or implied'.

Express consent – refers to consent that is clearly and unmistakably stated, and can be obtained either in writing, orally, or in any other form where the consent is clearly communicated.

As a general rule, if a health service provider needs or wants consent and is in doubt about whether an individual is giving consent or not, it is preferable to seek express consent.

Implied consent – there are situations when health service providers may reasonably rely on implied consent by individuals to handle health information in certain ways.

For example, an individual presents to a medical practitioner, discloses health information, and this is written down by the practitioner during the consultation – this will generally be regarded as giving implied consent to the practitioner to collect the information for certain purposes. The extent of these purposes will usually be evident from the discussion during the consultation.

Similarly, if a medical practitioner collects a specimen to send to a pathology laboratory for testing, it would be reasonable to consider that the individual is giving implied consent to the passing of necessary information to that laboratory

Where there is open communication and information sharing between the health service provider and the individual, consent issues will usually be addressed during the course of the consultation. If the discussion has provided the individual with an understanding about how their health information may be used, then it would be reasonable for the health service provider to rely on implied consent.

Where consent is required from individuals for the collection and use of data for public health purposes, such as in relation to the establishment and maintenance of a disease register, it may sometimes be appropriate to take the approach of giving individuals the opportunity to opt out of being included on the register. The use of this approach by a health service provider would only be appropriate where individuals are clearly informed about the option to opt out and this is prominently presented and easy to adopt.

(Guidelines on Privacy in the Private Health Sector, OFPC, November 2001, pp. xiv–xv)

The guidelines confine implied consent to situations where the circumstances make it clear that information is being collected and for what purpose. There appears little scope for extending the meaning of implied consent to allow research use of health information where the circumstances of its collection would not support a clear implication that it will be so used.

The inclusion of the possibility of implied consent needs to be compared with the requirements of the National Statement, paragraphs 1.7 and 1.9. These require that there be consent to participation in research, that it be informed and voluntary and that research be so designed that "each participant's consent is clearly established."

Collection without consent

Sensitive, and therefore health, information can be collected without the consent of the individual, if required by law, if necessary to prevent a serious and imminent threat to a person's life or health and that person cannot consent, for purposes of non-profit organisations and for legal claims. NPP 10 further provides that health information can be collected if it is necessary to provide a health service to the individual and is done in accordance with law or professional standards as to confidentiality. Here it is relevant to bear in mind NPP 1.4 which provides that if it is reasonable and practicable, organisations must collect information about an individual from that individual.

Where it is collected from a third person, NPP 1.5 requires the collector to inform the person whose information it is of certain matters. Inadvertent breaches of this NPP may occur in the course of collecting genetic information or family histories. The Privacy Commissioner has issued Public Interest Determinations that permit the collection of personal information about others without their consent, but only for the purposes of providing a health service to the person from whom the information is sought. They would not accordingly authorise the collection of such information in a research project with the result that such a collection would need to be approved by an HREC relying on the guidelines approved for the purposes of NPP 10.3.

Section 95A

NPP 10.3 permits collection of health information necessary for any of three purposes if:

1. that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
2. it is impracticable for the organisation to seek the individual's consent to the collection; and
3. the information is collected:
   (i) as required by law (other than this Act); or
   (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
   (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

The three purposes are research or the compilation of statistics or analysis of statistics, all relevant to public health or public safety, and the management, funding or monitoring of a health service.

The guidelines – *Guidelines Approved under Section 95A of the Privacy Act* 1988 – parallel to an extent those issued under section 95 of the Act. The guidelines are, however, a more complex document because they provide guidance on the collection, use and disclosure of health information for each of the three permitted purposes and, as well, because they use the mechanism of an HREC to review proposals for such collection, use or disclosure they also contain a section identifying the factors that an HREC must take into account. As with the section 95 guidelines, the central decision that an HREC is required to make is whether the public interest in the proposed activity does or does not outweigh the public interest in the protection of privacy.

Impracticable

The need to use the guidelines only arises when the other conditions in NPP 10.3 are met, namely, that the information is necessary for the purpose, the purpose cannot be served by collecting non-personal information and it is impracticable for the organisation to seek the individual's consent. No guidance is provided on the first two of these, but at page 24 of the Guidelines on Privacy in the Private Health Sector, it is said:

"Whether it is impracticable to seek consent will depend on the particular circumstances of the case. Simply incurring some expense, or having to exercise some effort to seek the consent of individuals whose information is to be used or disclosed, would not ordinarily make it 'impracticable' to seek consent. Circumstances where it may be impracticable to seek consent could include where there are no current contact details for the individuals in question and where there is insufficient information to get up-to-date contact details. This might occur in longitudinal studies of old records".

HREC approval

The section 95A guidelines, at pages 13–14, then require the person seeking to collect health information to seek the approval of an HREC for that collection and to give the HREC the following detailed set of information:

Guidance for preparing a written proposal to be submitted to an HREC

A.2.6 In the proposal to collect health information for the purpose of research relevant to public health or public safety, the collector(s) should state:

(a) the aims or purpose of the collection;

(b) the credentials and technical competence of the collector(s) of the data;

(c) the data needed;

(d) the study period;

(e) the target population;

(f) the reasons why de-identified information can not achieve the relevant purpose of the research activity;

(g) the reasons why it is impracticable to seek consent from the individual for the collection of health information;

(h) the estimated time of retention of the health information;

(i) the identity of the custodian(s) of the health information collected;

(j) the security standards to be applied to the health information. Standards must be in accordance with NPP 4. (See: Appendix 1). [Note: In particular, health information should be retained in accordance with the *Joint NHMRC/AVCC Statement and Guidelines on Research Practice* (See: Appendix 3), and in a form that is at least as secure as it was in the sources from which the health information was obtained unless more stringent legislative or contractual provisions apply];

(k) a list of personnel within the collecting organisation or organisations with access to the health information collected;

(l) the level of protection that will be applied by the collector(s) to protect health information disclosed to the collector(s) by the disclosing organisation. These should include:

(i) terms of any release agreement between the disclosing organisation and the collector(s) to govern limits on the use and disclosure of collected health information. [See: paragraph A.2.9 of these guidelines]; and

(ii) proposed methods of disposal of the health information on the completion of the research activity, as required by NPP 4.2. (See: Appendix 1).

A.2.7 The collector(s) of health information for the purpose of research relevant to public health or public safety should provide to the organisation(s) from which health information is sought, written notification of the decision of the HREC made in accordance with these guidelines. This written notification

removes the obligation for the disclosing organisation(s) to submit a written proposal to an HREC to disclose health information for the same research activity. [See: paragraph A.3.5 of these guidelines]. A disclosing organisation may still decide to submit a written proposal to an HREC in accordance with section A.3 of these guidelines even if that disclosing organisation receives written notification of HREC approval from the collector(s).

A.2.8 The collector(s) of health information for the purpose of research relevant to public health or public safety must immediately report to the HREC anything that might warrant review of ethical approval of the research proposal. [See: paragraph 2.37, 'Human Research Ethics Committees' *National Statement* (1999)].

A.2.9 Disclosure of health information collected under these guidelines, and therefore collected in accordance with NPP 10.3, must be in accordance with NPP 10.4. (See: Appendix 1). [See: OFPC Information Sheet 9–2001 *Handling health information for research and management* for further information on privacy obligations required under NPP 10.4].

A.2.10 Once a proposal submitted to an HREC to collect health information for the purpose of research relevant to public health or public safety satisfies the procedural requirements outlined in this section (A.2), the HREC must then weigh the public interest considerations set out in section D.5 of these guidelines.

As with the list in the section 95 guidelines, this is a daunting requirement for applicants. When it is embedded in a document that provides similar lists for collection for the two other purposes (in addition to lists for the use or disclosure of health information for either of the first two purposes), the difficulty and complexity seems greater. It may be that these requirements have dissuaded the pursuit of some research proposals.

HRECs are directed to have regard to a common set of matters whether the decision they are being asked to make relates to the collection, use or disclosure of health information and regardless of which of the three purposes is relevant. The list is set out in Part D of the Guidelines on pages 29–31:

D. Consideration by human research ethics committees (HRECs)

D.1 Before making a decision under these guidelines, an HREC must assess whether it has sufficient information, expertise and understanding of privacy issues, either amongst the members of the HREC or otherwise available to it, to make a decision that takes proper account of privacy matters. For the review of proposals for the collection of health information for the purpose of health service management, this may necessitate the appointment of additional members with specific expertise in the management, funding or monitoring of a health service. [See: '2. Human Research Ethics Committees' and '18. Privacy of Information', *National Statement* (1999)].

D.2 In making decisions under these guidelines, an HREC must consider whether the proposal complies with the relevant NPPs in the course of:

(a) the collection of health information for the purposes of:

(i) research relevant to public health or public safety; or

(ii) the compilation or analysis of statistics, relevant to public health or public safety; or

(iii) the management, funding or monitoring of a health service; or

(b) the use and disclosure of health information for the purposes of:

(i) research relevant to public health or public safety; or

(ii) the compilation or analysis of statistics, relevant to public health or public safety.

This would include considering whether the purpose of the proposed activity can be achieved using de-identified data and whether it is impracticable to collect, use or disclose health information for the proposed activity with the consent of the individual(s) involved.

D.3 In making decisions under these guidelines the HREC must ensure that the committee has the competence to determine if the public interest in the proposed activity substantially outweighs, or does not substantially outweigh, the public interest in the protection of privacy.

D.4 If the public interest in the proposed research, or compilation or analysis of statistics, or health service management activity does not substantially outweigh the public interest in the protection of privacy, then the activity should not be approved to proceed by the HREC.

Weighing the public interest

D.5 In determining whether the public interest in the proposed activity substantially outweighs, or does not substantially outweigh, the public interest in the protection of privacy, an HREC should consider the following matters:

(a) the degree to which the proposed collection, use or disclosure of health information is necessary to the functions or activities of the organisation;

(b) the degree to which the research, or compilation or analysis of statistics activity is relevant to public health or public safety;

(c) the degree to which the research, or compilation or analysis of statistics or the health service management activity is likely to contribute to :

(i) the identification, prevention or treatment of illness, injury or disease; or

(ii) scientific understanding relating to public health or safety; or

(iii) the protection of the health of individuals and/or communities; or

(iv) the improved delivery of health services; or

(v) enhanced scientific understanding or knowledge; or

(vi) enhanced knowledge of issues within the fields of social science and the humanities relating to public health or public safety;

(d) any likely benefits to individuals, to the category of persons to which they belong, or the wider community that will arise from the research, or compilation or analysis of statistics, or management of a health service being undertaken in the manner proposed;

(e) in considering benefits to the category of persons to which the individual(s) belong, specific consideration should be given to any likely benefits to individuals that belong to certain categories where the information may be of a particularly personal or sensitive nature; for example:

  (i) children and young people; or

  (ii) persons with intellectual or psychiatric disability; or

  (iii) persons highly dependent on medical care; or

  (iv) persons in dependent or unequal relationships; or

  (v) persons who are members of collectivities; or

  (vi) Aboriginal and Torres Strait Islander peoples; or

  (vii) persons whose information relates to their mental or sexual health; [See: *National Statement* for further information on considerations relevant to the above categories of persons.];

(f) whether the research, or compilation or analysis of statistics, or management of a health service study design can be satisfied without needing to apply NPP 2.1(d)(ii) and/or NPP 10.3(d)(iii) and the scientific defects in the activity that might arise if the activity was not undertaken in the manner proposed;

(g) the cost of not undertaking the research, or compilation or analysis of statistics, or management of a health service activity (to government, the public, the health care system etc);

(h) the public importance of the proposed research, or compilation or analysis of statistics, or management of a health service activity;

(i) the extent to which the data being sought are usually available to the public from the organisation that holds that data; and

  (i) whether the research, or compilation or analysis of statistics activity, involves use of the data in a way that is inconsistent with the purpose for which the data was made public; and

  (ii) whether the research, or compilation or analysis of statistics activity requires alteration of the format of the data of a kind that would, if used or disclosed by an organisation, involve a breach of an NPP;

(j) whether the risk of harm to an individual whose health information is to be collected, used or disclosed in the proposed research, or compilation or analysis of statistics, or management of health service activity is minimal, based on the information provided in proposals submitted under paragraphs A.2.6; or A.3.6; or B.2.6; or B.3.6; or C.2.6 of these guidelines;

(k) the standards of conduct that are to be observed in the research, or compilation or analysis of statistics, or management of a health service activity, including:

(i) the study design and the scientific credentials of those involved in conducting that study;

(ii) if the study involves contact with participants, the procedures or controls that will apply to ensure that participants are treated with integrity and sensitivity, including whether questions to be asked or procedures to be employed are intrusive;

(iii) whether access to health information is adequately restricted to appropriate personnel involved in conducting the proposed study;

(iv) the procedures that are to be followed to ensure that the health information is permanently de-identified before the publication of results;

(v) the procedures that are to be followed at the completion of the proposed study to ensure that all data containing health information are at least as secure as they were in the sources from which the data was obtained, including the date when the data will be destroyed or returned. These procedures must be in accordance with NPP 4 (See: Appendix 1).

The list is provided to show the complexity involved. As with the section 95 guidelines, a matter for NHMRC is whether it is within the intended competence of HRECs to determine issues of privacy – to be satisfied, as these guidelines require, that they have expertise to assess such issues. If these are not conventionally regarded as matters for research ethics, issues for the NHMRC include the effect on the other responsibilities of HRECs of the imposition of this responsibility and the question of why HRECs should have this obligation imposed on them. The public interest may be better served if the section 95A guidelines identified more concisely the matters to be weighed.

HREC experience

Early returns from the use of these guidelines by HRECs, as to collection, use and disclosure, shows that between December 2001 and June 2002, 52 HRECs reported a use of or reference to the section 95A guidelines in their consideration of 712 protocols. However, a closer investigation showed that of the 712 proposals, only 97 needed to be assessed using the guidelines. The other projects involved collection, use or disclosure with consent, or used de-identified information or involved organisations not in the private sector. There remained 25 HRECs involved in the assessment of the 97 proposals, of which 49 were for research, 24 for statistical purpose and 24 for monitoring a health service.

Use and Disclosure under the NPPs

The NPPs permit the use or disclosure of health information for a purpose directly related to the purpose for which it was collected and that is within the reasonable expectation of the individual. There is no statutory guide for the meaning of this expression but the Privacy Commissioner has, under section 27 of the Privacy Act, issued advisory Guidelines on Privacy in the Private Health Sector. These indicate that directly related secondary purposes in the health sector include:

- providing an individual with further information about treatment options;
- billing or debt-recovery;
- an organisation's management, funding, service-monitoring, complaint-handling, planning, evaluation and accreditation activities – for example, activities to assess the cost effectiveness of a particular treatment or service;
- disclosure to a medical expert (only for medico-legal opinion), insurer, medical defence organisation, or lawyer, solely for the purpose of addressing liability indemnity arrangements, for example in reporting an adverse incident.
- disclosure to a lawyer for the defence of anticipated or existing legal proceedings;
- an organisation's quality assurance or clinical audit activities, where they evaluate and seek to improve the delivery of a particular treatment or service; and
- disclosure to a clinical supervisor by a psychiatrist, psychologist or social worker.

(Guidelines on Privacy in the Private Health Sector, OFPC, November 2001, p. 19)

Potential Impingement on the NHMRC

(a) Activities that it promotes

The implication for the NHMRC's support of research is that a health service provider who has collected health information for a purpose other than research, typically diagnosis or treatment, and now wishes to use the information for research cannot do so without consent or HREC review and approval.

NPP 2 thus prohibits some previously routine health care provider practices, eg the practice of perusing weekly hospital admission records to identify persons who may be eligible for invitation to join current research projects, and even such a perusing of patient records by a general practitioner. The consequence, that may appear pedantic, is that health service providers need to seek the consent of patients before the provider reviews their information for research purposes. While most patients might find this unnecessary, it is probably equally true that they would not reasonably expect the provider to use their information in that way without their consent. Perhaps a practice of routinely seeking consent to review health information in order to decide whether to seek consent to use it in research may address this.

Use and Disclosure with Consent

If the proposed purpose of the use or disclosure is not directly related to the purpose of collection, consent will ensure compliance with NPP 2. As noted above, consent is defined as including express and implied consent. Guidance on the meaning of that definition, noted above, shows that implied consent is interpreted narrowly and does not remove the need for a consent process for research use of health information collected for diagnosis or treatment.

It will be unusual that consent for use of information in research will have been gained at the time the information is collected for diagnosis/treatment. Further, to seek such consent in a way that is not specific to the research would be contrary to the National Statement, paragraph 1.7. A change in health care provider practices to seek comprehensive (sometimes called "blanket") consent for research use of information collected for treatment may meet the requirements of NPP 2 but would not conform to the present wording of the National Statement.

HREC Approval

The remaining option for use, for research or related purposes, of health information collected for unrelated purposes is provided by NPP 2.1(d). This allows use or disclosure of health information for an unrelated purpose if three conditions are met:

1. it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
2. the use or disclosure is conducted in accordance with guidelines approved by the Federal Privacy Commissioner under section 95A for the purposes of this subparagraph; and
3. in the case of disclosure – the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information;

Guidance on the meaning of "impracticable" has been noted above and is applicable here.

The requirement in 3 is, in effect, re-inforced by the requirement in NPP 10.4 that the recipient (now a "collector") "must take reasonable steps to permanently de-identify the information before the organisation discloses it". This appears to limit the ongoing exchange of information, even of coded information (which is not permanently de-identified), that is necessary for linking databases.

As with collection, the section 95A guidelines provide a detailed list of matters that an applicant must provide to an HREC. The list is similar in length and demand to that extracted above in relation to collection and raises similar issues as to its dissuading effect.

PART FOUR

STATES/TERRITORIES WITH PRIVATE SECTOR PRIVACY REGULATION

Two Australian States and one Territory have enacted legislation to protect privacy in the handling of health information in the private sector. Victorian and ACT legislation is in force and that in NSW is expected to be in force early in 2004.

In these jurisdictions, the difficulty facing handlers of health information is that both the Federal Privacy Act, for reasons noted above, and the local legislation applies. If they are not identical, it may be a complex or burdensome task to comply with both.

AUSTRALIAN CAPITAL TERRITORY

The *Health Records (Privacy and Access) Act 1997* (ACT) is primarily designed to regulate the handling of health information for the treatment of health consumers. It regulates a narrower range of conduct than does the Federal Privacy Act.

Collection

By use of privacy principles, the Act prohibits, in section 5, a collector from collecting personal health information for inclusion in a health record unless-

(a) the information is collected for a lawful purpose that is 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.

The definitions in section 4 of collector, health record and health service indicate the scope of the regulation:

"**collector** means:

a person who, in the course of his or her profession, employment or official duty, collects personal health information;

"**health record** means: any record-

(a) held by a health service provider and containing personal information; or

(b) containing personal health information; and includes a part, or parts, of such a record";

"**health service** means:

(a) any activity that is intended or claimed (expressly or by implication), by the person performing it, to assess, record, improve or maintain the physical, mental or emotional health of a consumer or to diagnose or treat an illness or disability of a consumer; or

(b) a disability, palliative care or aged care service that involves the making or keeping of personal health information; but does not include any service that, under the regulations, is an exempt service";

"**health service provider** means:

a person (including a body corporate, government agency or other body) that provides a health service in the Territory".

The principles bind persons who collect personal health information in the course of their profession and so may include professional health researchers but may exclude others. Further, the principle only governs collection for inclusion in a health record, the definition of which confines it to health service providers in the Territory. Such people would comply with the Privacy Act if collecting health information under the ACT Act. Other persons (not being those who collect such information in their profession) or other collections (not for inclusion in a health record) appear not to be subject to the ACT Act.

Use

Principle 9 (in section 5) regulates the use of personal health information by permitting it to be shared between members of a treating team to the extent necessary to improve or maintain the consumer's health or to manage a disability of the consumer, but prohibits a record-keeper who has possession or control of a health record that was obtained for a particular purpose from using the information for any other purpose unless-

(a) the consumer has consented to use of the information for that other purpose;

(b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a significant risk to the life or physical, mental or emotional health of the consumer or another person;

(c) use of the information for that other purpose is required or authorised by-

(i) a law of the Territory;

(ii) a law of the Commonwealth; or

(iii) an order of a court of competent jurisdiction;

(d) the purpose for which the information is used is directly related to the purpose for which the information was obtained; or

(e) the use of the information is related to the management, funding or quality of the health service received by the consumer.

The principle binds only a record keeper who is defined as a person (including a body corporate, government agency or other body) that has possession or control of a health record, the definition of which in turn confines it to ACT health service provision.

Further it only binds in relation to a consumer, defined in section 4 to relate it to the definitions of health record and health service:

"**consumer** means: an individual-

(a) who uses, or has used, a health service; or

(b) in relation to whom a health record has been created; and includes-

(c) a person authorised by the consumer under subsection 13 (7) to have access to the health record;

(d) where the consumer is a young person or a legally incompetent person – a guardian of the consumer; and (e) where the consumer has died – a legal representative of the deceased consumer";

Potential Impingement on the NHMRC

(a) Activities that the NHMRC promotes

The apparent potential impingement for the NHMRC is that access, for research purposes, to personal health information held in records by ACT health service providers is only available with consent of the individuals. The principles do not permit a record holder to use the information for an unrelated purpose on the basis of an HREC review. However, the provisions of sub-clause (c), referring to authorisation of other uses by a law of the Commonwealth, would appear to allow such access, provided it follows the Federal Privacy Act provisions.

Disclosure

Similarly with disclosure. Principle 10 (in section 5) provides that;

Except where personal health information is being shared between members of a treating team only to the extent necessary to improve or maintain the consumer's health or manage a disability of the consumer, a record-keeper who has possession or control of a health record shall not disclose the information to a person or agency (other than the consumer) unless-

(a) the consumer is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person or agency;

(b) the consumer has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent risk to the life or physical, mental or emotional health of the consumer or of another person;

(d) the disclosure is required or authorised by-

  (i) a law of the Territory (including this Act);

  (ii) a law of the Commonwealth; or

  (iii) an order of a court of competent jurisdiction; or

(e) the disclosure of the information is necessary for the management, funding or quality of the health service received by the consumer.

The principle recognises that authorisation of disclosure by a law of the Commonwealth would permit a disclosure, without consent or awareness of a consumer, when the guidelines approved under section 95A of the Privacy Act are followed.

VICTORIA

The *Health Records Act 2001* came into force on 1 July 2002 and governs the handling of health information by both public and private sector entities.

Scope

As with the Federal Privacy Act, this is determined by the key definitions of personal and health information and entities that are bound.

Personal information is defined in section 3 in almost identical terms to that in the Federal Privacy Act, with the addition of information about deceased people for 30 years after their death:

"personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information about an individual who has been dead for more than 30 years".

Health information defined in section 3 is again similar but broader than the definition in the Federal Act particularly with the explicit inclusion of genetic information:

"**health information** means:

(a) information or an opinion about-
  (i) the physical, mental or psychological health (at any time) of an individual; or
  (ii) a disability (at any time) of an individual; or
  (iii) an individual's expressed wishes about the future provision of health services to him or her; or
  (iv) a health service provided, or to be provided, to an individual – that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants – but does not include health information, or a class of health information or health

information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act";

The definition of health service in section 3 is also relevant:

"**health service** means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the organisation performing it-

(i) to assess, maintain or improve the individual's health; or

(ii) to diagnose the individual's illness, injury or disability; or

(iii) to treat the individual's illness, injury or disability or suspected illness, injury or disability; or

(b) a disability service, palliative care service or aged care service; or

(c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist; or

(d) a service, or a class of service, provided in conjunction with an activity or service referred to in paragraph (a), (b) or (c) that is prescribed as a health service – but does not include a health service, or a class of health service, that is prescribed as an exempt health service for the purposes of this Act generally or for the purposes of specified provisions of this Act or to the extent that it is prescribed as an exempt health service".

The Act applies to any public and private sector entity that is a health service provider or collects, holds or uses health information. These entities are required to handle that information in accordance with 11 Health Privacy Principles contained in a Schedule to the Act.

Collection

HPP 1 applies to the collection of health information after the commencement of the Act. The principle sets out the circumstances in which health information can be collected:

An organisation must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and at least one of the following applies-

(a) the individual has consented;

(b) the collection is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law);

(c) the information is necessary to provide a health service to the individual and the individual is incapable of giving consent within the meaning of section 85(3) and-

(i) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or

(ii) the individual does not have such an authorised representative;

(d) the information is disclosed to the organisation in accordance with HPP 2.2(a), (f), (i) or (l) or HPP 2.5;

(e) if the collection is necessary for research, or the compilation or analysis of statistics, in the public interest-

(i) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(ii) it is impracticable for the organisation to seek the individual's consent to the collection; and

(iii) the information is collected in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this sub-paragraph;

(f) the collection is necessary to prevent or lessen

(i) a serious and imminent threat to the life, health, safety or welfare of any individual; or

(ii) a serious threat to public health, public safety or public welfare – and the information is collected in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph;

(g) the collection is by or on behalf of a law enforcement agency and the organisation reasonably believes that the collection is necessary for a law enforcement function;

(h) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;

(i) the collection is in the prescribed circumstances.

The conditions are substantially the same as in the NPPs, although some differences merit noting. The definition of research or statistics, is to those activities "in the public interest" a broader concept than the "relevant to public health and public safety" used in the Federal Privacy Act.

One consequence for NHMRC of this is that collection for research in the public interest in Victoria may not be regarded as collection for research relevant to public health and safety under the Federal Act, triggering a possible complaint to the Federal Privacy Commissioner about a breach of NPP 1. Additionally, the collection of information about a deceased person within 30 years of their death is governed by the Victorian Act but not by the Federal Act.

Collection for research without consent is, like the Federal Privacy Act, dependent on the purpose not being able to be met by the collection of non-identifying information and it being impracticable to seek consent. The guidelines issued under section 22

make specific and helpful reference to the risk of differences between the Federal and State regulation:

"Conscious of these facts and the need to ensure, as far as the Act allows, a level of consistency across the requirements with which researchers and organisations must already comply, the Commissioner has, for her statutory research guidelines, drawn on those issued by the NHMRC for the purposes of sections 95 and 95A of the Privacy Act which, in turn, make substantial reference to the *National Statement*.

There are some inevitable differences. The section 95 guidelines must refer back to, and be grounded in, the language and the scope of the section of the Privacy Act under which they are made. The section 95 guidelines deal, for example, with "medical research", while the section 95A guidelines apply to research and statistical compilation and analysis which is "relevant to public health and public safety", as well as to collection of health information without consent for the purpose of the management, funding or monitoring of a health service. In contrast, Victoria's HPPs deal with research and statistical compilation and analysis "in the public interest".

The differences to be found in the Health Services Commissioner's guidelines serve only to ensure they reflect the objectives and requirements of the *Health Records Act* 2001 (Vic), the legislation of which they are a part. Those who know and work with the current NHMRC guidelines will find much that is familiar in the spirit and content of these guidelines."

(Statutory Guidelines on Research, Office of the Health Services Commissioner (Victoria) 2002, p.7)

There is also a table comparing the differences with attention to the work of HRECs in assessing proposals and reporting their decisions. The Victorian guidelines closely follow those issued under section 95A of the Federal Privacy Act, with differences being matters of reference to the Victorian legislation. It follows that where HREC approval is needed for collection (and for use and disclosure) of health information for research or statistical purposes, procedural conformity with the Victorian guidelines will meet the requirements of the Section 95A guidelines. HRECs will need to provide an annual report of their decisions to the Victorian Health Services Commissioner, as required by the Victorian guidelines, paragraph 4.8–4.9, but the information contained in that report would be practically identical to that required by the annual reporting to the Australian Health Ethics Committee under the Federal Privacy Act.

Use and disclosure

Health Privacy Principle 2 contains a list of circumstances when health information can be used or disclosed:

2. Principle 2 – Use and Disclosure

2.1 An organisation may use or disclose health information about an individual for the primary purpose for which the information was collected in accordance with HPP 1.1.

2.2 An organisation must not use or disclose health information about an individual for a purpose (the "secondary purpose") other than the primary purpose for which the information was collected unless at least one of the following paragraphs applies:

(a) both of the following apply

(i) the secondary purpose is directly related to the primary purpose; and

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) the use or disclosure is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law); or

(d) all of the following apply

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use or disclosure for the secondary purpose is reasonably necessary for the provision of the health service; and

(iii) the individual is incapable of giving consent within the meaning of section 85(3) and

(A) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or

(B) the individual does not have such an authorised representative; or

(e) all of the following apply

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use is for the purpose of the provision of further health services to the individual by the organisation; and

(iii) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively; and

(iv) the information is used in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(f) the use or disclosure is for the purpose of:

(i) funding, management, planning, monitoring, improvement or evaluation of health services; or

(ii) training provided by a health service provider to employees or persons working with the organisation, and

(iii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which

the individual's identity cannot reasonably be ascertained and it is impracticable for
the organisation to seek the individual's consent to the use or disclosure; or

(iv) reasonable steps are taken to de-identify the information, and

(v) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(vi) the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this sub-paragraph; or

(g) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(iii) the use or disclosure is in accordance with guidelines issued or approved by the Health Services Commissioner under section 22 for the purposes of this sub-paragraph; and

(iv) in the case of disclosure

(A) the organisation reasonably believes that the recipient of the health information will not disclose the health information; and

(B) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained; or

(h) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent

(i) a serious and imminent threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health, public safety or public welfare – and the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Services Commissioner under section 22 for the purposes of this paragraph; or

(i) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities and, if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence; or

(j) the organisation reasonably believes that the use or disclosure is reasonably necessary for a law enforcement function by or on behalf of a law enforcement agency and, if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence; or

(k) the use or disclosure is necessary for the establishment, exercise or defence of a legal or equitable claim; or

(l) the use or disclosure is in the prescribed circumstances.

Note: Nothing in HPP 2 requires an organisation to disclose health information about an individual. An organisation is always entitled not to disclose health information in the absence of a legal obligation to disclose it.

These authorisations are broader than those contained in the *Privacy Act*, but those that relate to the interests of NHMRC, especially research, are substantially the same. The guidelines issued for the purpose of paragraph 2.2 (g) are, as noted above, substantially the same as those approved under section 95A of the Federal Privacy Act.

One authorised disclosure of health information that is wider than that in the Federal Act is in HPP 2.4 which allows disclosure to third parties for the provision of health care or for compassionate reasons. There is no comparable provision in the Federal Act and the recommendations 21–1 and 21–2 in *Essentially Yours** recognised this issue. It is an example of a more open approach to ethical practice in the handling of health information.

2.4 Despite HPP 2.2, a health service provider may disclose health information about an individual to an immediate family member of the individual if-

(a) either-

(i) the disclosure is necessary to provide appropriate health services to or care of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(b) the disclosure is limited to the extent reasonable and necessary for the purposes mentioned in paragraph (a); and

(c) the individual is incapable of giving consent to the disclosure within the meaning of section 85(3); and

(d) the disclosure is not contrary to any wish -

(i) expressed by the individual before the individual became incapable of giving consent and not changed or withdrawn by the individual before then; and

(ii) of which the organisation is aware or could be made aware by taking reasonable steps; and

(e) in the case of an immediate family member who is under the age of 18 years, considering the circumstances of the disclosure, the immediate family member has sufficient maturity to receive the information.

* *Essentially Yours. The protection of human genetic information in Australia.* Australia Law Reform Commission/National Health and Medical Research Council, 2003 (pp565,570)

NEW SOUTH WALES

Health Records and Information Privacy Act 2002

This Act is not yet in force but is expected to commence early in 2004.

The Act is aimed to promote fair and responsible handling of health information by:

(a) protecting the privacy of an individual's health information that is held in the public and private sectors, and

(b) enabling individuals to gain access to their health information, and

(c) providing an accessible framework for the resolution of complaints regarding the handling of health information.

The objects are expressed to be:

(a) to balance the public interest in protecting the privacy of health information with the public interest in the legitimate use of that information, and

(b) to enhance the ability of individuals to be informed about their health care, and

(c) to promote the provision of quality health services.

(Health Records and Information Privacy Act 2002 (NSW) S.3)

Scope

The Act applies a set of health privacy principles (HPPs) to all private sector persons and public sector agencies that are health service providers or who collect, hold or use health information.

The definition of public sector agencies is the same as that used in the *Privacy and Personal Information Protection Act 1998 (NSW)* and the definition of private sector persons is comprehensive.

The definitions of health service provider and health service in section 4 are similar to the Victorian legislation.

Health service provider means an organisation that provides a health service but does not include:

(a) a health service provider, or a class of health service providers, that is prescribed by the regulations as an exempt health service provider:

  (i) for the purposes of this Act generally, or

  (ii) for the purposes of specified provisions of this Act, or

  (iii) for the purposes of specified Health Privacy Principles or health privacy codes of practice, or

  (iv) to the extent to which it is prescribed by the regulations as an exempt health service provider, or

(b) an organisation that merely arranges for a health service to be provided to an individual by another organisation

Health service includes the following services, whether provided as public or private services:

(a) medical, hospital and nursing services,

(b) dental services,

(c) mental health services,

(d) pharmaceutical services,

(e) ambulance services,

(f) community health services,

(g) health education services,

(h) welfare services necessary to implement any services referred to in paragraphs (a)–(g),

(i) services provided by podiatrists, chiropractors, osteopaths, optometrists, physiotherapists, psychologists and optical dispensers in the course of providing health care,

(j) services provided by dietitians, masseurs, naturopaths, acupuncturists, occupational therapists, speech therapists, audiologists, audiometrists and radiographers in the course of providing health care,

(k) services provided in other alternative health care fields in the course of providing health care,

(l) a service prescribed by the regulations as a health service for the purposes of this Act.

Likewise the definition of health information in section 6 is similar to that in the Federal Privacy Act but, as in Victoria, includes explicitly genetic information and, because the NSW Act draws on the VIC definition of personal information includes information about a person for 30 years after their death:

"**health information** means:

(a) personal information that is information or an opinion about:

(i) the physical or mental health or a disability (at any time) of an individual, or

(ii) an individual's express wishes about the future provision of health services to him or her, or

(iii) a health service provided, or to be provided, to an individual, or

(b) other personal information collected to provide, or in providing, a health service, or

(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or

(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual,

but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act".

The Act applies 12 Health Privacy Principles in a Schedule to the Act to those private sector persons and public sector agencies about their handling of that information. The principles on collection are substantially the same as the corresponding NPPs in the Privacy Act.

There are two provisions of note, sections 9 and 10, that are related to collection. These establish when a person or agency "holds" health information:

9. For the purposes of this Act, health information is held by an organisation if:
   (a) the organisation is in possession or control of the information (whether or not the information is contained in a document that is outside New South Wales), or
   (b) the information is in the possession or control of a person employed or engaged by the organisation in the course of such employment or engagement, or
   (c) in the case of a public sector agency – the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.

10. For the purposes of this Act, health information is not collected by an organisation if the receipt of the information by the organisation is unsolicited.

As to use and disclosure, HPPs 10 and 11, follow similar patterns to those in the Victorian legislation, but appear to introduce some relaxation of use and disclosure for health services, training and research, (as well as other purposes) as to which they are reproduced:

10 Limits on use of health information

(1) An organisation that holds health information must not use the information for a purpose (a secondary purpose) other than the purpose (the primary purpose) for which it was collected unless:
   (a) the individual to whom the information relates has consented to the use of the information for that secondary purpose, or
   (b) the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose, or
   Note: For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.
   (c) the use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or

(ii) a serious threat to public health or public safety, or

(d) the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or...

Paragraphs (g) to (k) follow as do sub-paragraphs (2) to (5)

11 Limits on disclosure of health information

(1) An organisation that holds health information must not disclose the information for a purpose (a secondary purpose) other than the purpose (the primary purpose) for which it was collected unless:

(a) the individual to whom the information relates has consented to the disclosure of the information for that secondary purpose, or

(b) the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or

Note: For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

Sub-paragraphs (c) to (e) are substantially the same as those in Principle 10, as is (f):

(f) the disclosure of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and

(ii) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained, and

(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) the disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and:

(i) the disclosure is limited to the extent reasonable for those compassionate reasons, and

(ii) the individual is incapable of giving consent to the disclosure of the information, and

(iii) the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps, and

(iv) if the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information,

Sub-paragraphs (h) to (i) follow as do paragraphs (2) to (5).

The wording of (d), (e) and (f) in both HPPs appear to permit use or disclosure for management of health services, training and research where either identifiable information is necessary and consent is impracticable OR reasonable steps are taken to de-identify the information. Although HREC approval is still needed, this appears to be a relevant change. The compassionate disclosure provision in HPP 11 (g) mirrors that in the Victorian HPPs.

Draft Statutory guidelines

The Health Privacy Principles refer to guidelines issued by the Privacy Commissioner relating to use and disclosure of health information for research, training and management of health services. Draft guidelines have been issued on each of these matters, and on collection of health information from third parties.

The draft guidelines relating to use and disclosure of health information for research closely follow the section 95A guidelines so far as they relate to use and disclosure for that purpose. They contain a definition of research as:

> "For the purposes of these statutory guidelines, *'research'* involves systematic investigation to establish facts, principles or knowledge, with a defining feature being the validity of its results."

Their basic structure is the same, relying on the review of an HREC of the proposal to use or disclose health information and determining whether the public interest in the research does or does not outweigh to a substantial degree the public interest in the protection of privacy. Similar matters are required to be provided in an application to an HREC and for the HRECs to have regard to.

The guidelines make clear recognition that a use and disclosure by an agency or organisation is also a collection by a collector and so address both activities. They also contain two presumptions to be applied by an HREC in reviewing applications: namely that any screening of potential subjects is to be conducted by the disclosing person or agency and that the collector is to be presumed not to use the information to contact individuals.

PART FIVE

STATE/TERRITORY LEGISLATION/REGULATION IN THE PUBLIC SECTOR

The relevance of the legislation and regulation described in this section is to identify any differences in use and disclosure restrictions either between or among Australian States and Territories or between private and public sectors in any State or Territory.

All Australian jurisdictions, including the Commonwealth, have enacted legislation that limits, usually by specifically prohibiting, the disclosure by public sector employees of information obtained in the course of their duties unless that disclosure is for the purpose of those duties. There is a very large quantity of this legislation and reliable collection is difficult. Accordingly, some examples are given for some States to indicate the range of typical provisions. They appear under the heading Confidentiality Provisions.

AUSTRALIAN CAPITAL TERRITORY

The *Privacy Act 1988* (Clth) applies the IPPs to the public sector in the ACT.

NEW SOUTH WALES

Confidentiality provisions

Examples include:

(a) section 22 of the *Health Administration Act 1982* that prohibits a person disclosing any information obtained through the administration of the Act or other relevant Act unless the disclosure is made:
- with the consent of the person who provided the information,
- in order to administer the Act
- for legal proceedings
- without other lawful excuse.

(b) section 75 of the *Public Health Act 1991* that renders disclosure of information obtained in connection with the administration of the Act an offence unless it is made with the consent of the person who provided the information, for the administration of the Act or for legal proceedings.

(c) section 42J of the *Public Health Act 1991* that permits in specified circumstances the disclosure of identifying particulars of a woman whose details are contained on the NSW Pap Test Register.

Privacy legislation

There are two statutes that govern information privacy in the public sector. These are the *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002.*

Privacy and Personal Information Protection Act 1998

Scope

The Act governs the conduct of public sector agencies in NSW. This is potentially a wider class than in some other states because of the inclusion of section 3(d) which includes in those agencies

> (d) a person or body in relation to whom, or to whose functions, an account is kept of administration or working expenses, if the account:
>
> (i) is part of the accounts prepared under the Public Finance and Audit Act 1983 , or
>
> (ii) is required by or under any Act to be audited by the Auditor-General, or
>
> (iii) is an account with respect to which the Auditor-General has powers under any law, or
>
> (iv) is an account with respect to which the Auditor-General may exercise powers under a law relating to the audit of accounts if requested to do so by a Minister of the Crown.

The definition of personal information in section 4, to which the protection is applied, is also broader than in the Privacy Act in two respects: the inclusion of tissue samples as information and of information about deceased people:

In this Act, personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

(2) Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

(3) Personal information does not include any of the following:

> (a) information about an individual who has been dead for more than 30 years, (other exclusions appear but are not noted)

The Act contains in sections 8–19 a set of information privacy principles. Those relating to collection, sections 8–11, are in substance the same as the corresponding IPPs. Those relating to use and disclosure are restrictive:

17 Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

> (a) the individual to whom the information relates has consented to the use of the information for that other purpose, or

(b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or

(c) the 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 to whom the information relates or of another person.

18 Limits on disclosure of personal information

(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or

(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or

(c) the agency 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 another person.

19 Special restrictions on disclosure of personal information

(1) A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

These principles confine use to consensual, directly related or emergency purposes and disclosure to directly related or emergency purposes. Section 19 confines the disclosure of health information to emergency situations only.

Section 41 of the Act provides for the issue of directions by the NSW Privacy Commissioner that exempt agencies from complying with the principles

41 The Privacy Commissioner

(1) The Privacy Commissioner, with the approval of the Minister, may make a written direction that:

(a) public sector agency is not required to comply with an information protection principle or a privacy code of practice, or

(b) the application of a principle or a code to a public sector agency is to be modified as specified in the direction.

(2) Any such direction has effect despite any other provision of this Act.

(3) The Privacy Commissioner is not to make a direction under this section unless the Privacy Commissioner is satisfied that the public interest in requiring the public sector agency to comply with the principle or code is outweighed by the public interest in the Privacy Commissioner making the direction.

Under this section the NSW Privacy Commissioner has issued a Direction On Disclosures Of Information By Public Sector Agencies For Research Purposes that is effective from 1 April 2003 to 31 December 2003, or until the making of a Privacy Code of Practice for Research, whichever is earlier.

This direction permits a relaxation of the requirements in three contexts. Each of these is repeated below, followed by the relaxation that applies to it.

Context One:

a) the disclosure by a public sector agency covered by this Direction purposes [sic] of personal information held by the agency for research where this would otherwise breach sections 18 or 19 of the Privacy and Personal Information Protection Act;

Relaxation One:

4. In the case of conduct referred to in paragraph 3(a) of this Direction an agency may reasonably depart from sections 18 and 19 of the Act, provided that it follows guidelines or policies of the agency covering the disclosure of personal information for research purposes which were established at 1 July 2000, or the proposed research has been approved by a committee established for the purpose of giving ethical approval to research projects after such a committee has considered the privacy implications of the collection and subsequent use of such information by the researcher in the absence of express consent.

Context Two:

b) the collections, storage, use, disclosure, provision of personal access to and alteration of personal information in records which are created by a person or organisation that is not a public sector agency but which are deposited with a public sector agency for purposes which include research;

Relaxation Two:

5. In the case of conduct referred to in paragraph 3(b) of this Direction an agency is not required to comply with sections 8, 9, 10, 13, 14, 15, 16,17,18 or 19 of the Act, provided that the agency takes such steps as a reasonable in the circumstances to protect the privacy of any person whose personal information is contained in deposited records.

Context Three:

c) the collection and use of personal information by an agency or part of an agency which has as a major function the collection of items of historical or cultural significance and the information is collected and used to provide

reference material in relation to collected items; but does not apply to the use by or on behalf of a public sector agency of personal information held by the agency for purposes which are lawful purposes directly related to a function or activity of the agency, including the assessment or evaluation of the operation of the agency or services provided by the agency.

Relaxation Three:

6. In the case of conduct referred to in paragraph 3(c) of this Direction a relevant agency may collect, use and disclose personal information otherwise than in accordance with sections 8, 9, 10, 14, 15, 17, 18 and 19 of the Act, provided that it adheres to a written policy on the protection of the privacy of such material.

This is a significant relaxation of the strict principles in sections 17, 18 and 19 in relation to activities that NHMRC promotes, namely, the use and disclosure of information for research. Because most NSW universities and all NSW health services are public sector agencies, the Direction is central to their contribution to research. However, this position will change in relation to health information when the NSW Health Records and Information Privacy Act comes into effect in 2004.

The Act also restricts the disclosure of personal information on public registers to a "purpose relating to the purpose of the register or the Act under which the register is kept" (section 57). People may seek to have their personal information on public registers suppressed and the Commissioner may permit this. The provisions in the Act about public registers prevail over the law under which the register was established (section 59).

Health Records and Information Privacy Act 2002 (NSW)

This Act, not yet in force but expected to be so early in 2004, applies to the collection and use of health information in both public and private sectors. The discussion of this Act appears in Part Four above and is not repeated here.

NORTHERN TERRITORY

The *Information Act 2003* governs the functions of access by citizens to government information, the management of archives and privacy. The objectives of the Act are stated in section 3 to be:

(a) to provide the Territory community with access to government information by-

  (i) making available to the public information about the operations of public sector organisations and, in particular, ensuring that rules and practices affecting members of the public in their dealings with public sector organisations are readily available to persons affected by those rules and practices; and

  (ii) creating a general right of access to information held by public sector organisations limited only in those circumstances where the disclosure of particular information would be contrary to the

public interest because its disclosure would have a prejudicial effect on essential public interests or on the private and business interests of persons in respect of whom information is held by public sector organisations;

(b) to protect the privacy of personal information held by public sector organisations by –

(i) providing individuals with a right of access to, and a right to request correction of, their personal information held by public sector organisations;

(ii) establishing a regime for the responsible collection and handling of personal information by public sector organisations; and

(iii) providing remedies for interference with the privacy of an individual's personal information;

(c) to establish an independent office holder, the Information Commissioner, to oversee the freedom of information and privacy provisions of this Act; and

(d) to promote efficient and accountable government through appropriate records and archives management by public sector organisations.

Scope

The Act, so far as it governs privacy, adopts in section 4 a simpler definition of personal information:

> "personal information means government information from which a person's identity is apparent or is reasonably able to be ascertained".

The definitions of health information and health service in section 4 follow the lead of the Victorian legislation:

"**health information** means:

(a) personal information about-

(i) the physical or mental health of a person;

(ii) a person's disability; or

(iii) the provision of a health service to a person, including the person's expressed wishes about that provision;

(b) personal information connected with the provision of a health service;

(c) personal information connected with the donation or intended donation by a person of his or her body parts, organs or bodily substances; or

(d) personal information that is genetic information about a person in a form that is, or could be, predictive about the person's health at any time";

"**health service** means:

(a) an activity performed in relation to a person that is intended or claimed (expressly or otherwise) by the person or body performing it to-

(i) assess, record, maintain or improve the person's health;

(ii) diagnose the person's illness or disability; or

(iii) treat the person's illness or disability or suspected illness or disability;

(b) a disability, palliative care or aged care service; or

(c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist";

The Information Act applies to all public sector agencies in the Territory, listed exhaustively in section 5.

The Information Act subjects those agencies to compliance with the Information Privacy Principles contained in a Schedule to the Act. These are in substantially the same form as the Victorian Information Privacy Act.

Collection

Information Privacy Principle 1 of this NT legislation is substantially the same as NPP 1 but Principle 10 contains a less strict provision in relation to collection of sensitive information, similar to that in Victoria:

10.2 Despite IPP 10.1, a public sector organisation may collect sensitive information about an individual if-

(a) the collection-

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or

(ii) is of information relating to an individual's racial or ethnic origin and is for the purpose of providing government funded targeted welfare or educational services;

(b) there is no other reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.

Use and Disclosure

The NT Information Privacy Principle 2 is almost identical to NPP 2 and is not reproduced. However, section 71 of the Act marks an important variation of this privacy principle in relation to research and statistics:

IPP 2 (Use and disclosure) does not apply in relation to the use or disclosure of personal information by a public sector organisation in connection with a function or activity of the organisation that involves compiling statistics or conducting research unless those statistics or that research is published in a form that identifies a person.

There appears to be no significant potential impingement on activities that NHMRC promotes from the legislation, which applies principles that are less restrictive than the Federal Privacy Act only to public sector agencies.

QUEENSLAND

Confidentiality provisions

Examples include the following sections of the *Health Act 1937:*

(a) section 49 requires all person administering the Act in relation to notifiable diseases to maintain secrecy as to that information.

(b) section 100E prohibits the chief executive or any person administering the Act from disclosing or making use of information gained except when authorised. The Chief Executive is authorised to disclose information contained on the Cancer Register, if it is in a form that is believed not to identify a person, to a contractor who is maintaining the register, to a person authorised to conduct research or studies or to the Commonwealth, another State or a Commonwealth authority, if considered to be in the public interest

(c) section 100FO prohibits disclosure of information on the Pap Smear Register unless used for the purposes of the Act.

(d) section 100I prohibits a person administering the peri-natal statistics from disclosing information unless authorised but permits the Chief Executive to disclose non-identifying information to a person authorised to conduct research.

Privacy Regulation

The Queensland government has adopted, by *Information Standard 42,* the IPPs from the Federal Privacy Act to govern the handling of personal information by all Queensland departments other than the Department of Health. That department has adopted, by *Information Standard 42As,* the NPPs to govern its handling of personal, sensitive and health information.

Accordingly, there will be no significant difference in relevant principles governing the conduct of activities that NHMRC promotes in Queensland from those that the Federal Privacy Act applies.

Guidelines on the IPPs and NPPs

The Queensland government has issued guidelines on the IPPs that explain their operation, and also on the NPPs, that draw from the *Guidelines on Privacy in the Private Health Sector* issued by the Federal Privacy Commissioner. Appendix 4 to these guidelines contains guidelines equivalent to those approved under section 95A of the Federal Privacy Act, on which reliance was placed in developing the Queensland guidelines. The Appendix 4 guidelines meet the purposes of NPP2(1)(a) and NPP 10.3(d).

In the guidelines on the NPPs, some important matters are identified and commented on:

de-identified information (page 8):

> The NPPs do not apply to de-identified information or statistical data sets which are non-identifiable (ie. would not allow individuals to be identified). In order for information to be considered non-identifiable, all identifiable references to the individual must be removed and the context and content of the remaining details must make it impossible to identify the individual. Where identification could occur because the information is, or can be, linked to other personal records on an individual, or where the subset of data is small enough to allow individuals to be recognised in a particular context, the data is considered to be identifiable.

collection from third parties (page 18):

> While the Department is not bound by the Privacy Act 1988, from a policy perspective it agrees with the determination and supports the Commissioner's decision. Accordingly, where personal information of third parties is collected by officers in the context of medical, or social medical history taking, Departmental officers are not required to inform third parties or to seek their consent to collection.

Disclosure of health information (page 23):

In summary, the following rules apply to the use and disclosure of health information:-

> Where health information has been collected in the context of providing a health service use and disclosure is governed by the duty of confidentiality in section 63 of the Health Services Act 1991. However, this does not govern situations where information is "used" without being "given" to any other person.
>
> Where health information has been collected through a statutory provision (for example, information provided to the Pap Smear Registry) then it will be subject to any statutory requirements relating to use and disclosure.
>
> Where section 63 does not apply and there are no statutory requirements relating to use and disclosure, NPP 2 will apply. For example, NPP2 applies to information provided in a medical certificate provided by a Departmental officer.
>
> Where there is any doubt surrounding whether or not health information can or should be used or disclosed, advice should be sought from senior management in the first instance.

Disclosure limitations

The importance of section 63 of the *Health Service Act 1991 (QLD)* is apparent. That section imposes limitations on disclosure of personal information by public sector agencies that override the NPPs in Information Standard 42A:

63 Confidentiality

(1) An officer, employee or agent of the department must not give to any other person, whether directly or indirectly, any information acquired by reason of being such an officer, employee or agent if a person who is receiving or has received a public sector health service could be identified from that information.

Maximum penalty – 50 penalty units.

(2) Subsection (1) does not apply-

(a) to the giving of any information that an officer, employee or agent is expressly authorised or permitted to give under this or any other Act or that is required by operation of law; or

(b) to the giving of information with the prior consent of the person to whom it relates or, if the person has died, with the consent of the person's spouse or, if the spouse is not reasonably available, the senior available next of kin of the person; or

(c) to the giving of information concerning the condition of a person who is a patient in, or is receiving health services from, a public sector health service if the information-

(i) is communicated in general terms by a health professional in accordance with the recognised standards of the relevant medical or other health profession; or

(ii) is communicated by a member of the medical staff of a public sector health service to the next of kin or a near relative, including a spouse, of the patient in accordance with the recognised standards of medical practice; or

(d) to the giving of information to the Australian Red Cross Society for the purpose of tracing blood, or blood products derived from blood, infected with any disease or the donor or recipient of any such blood; or

(e) to the giving of information required in connection with the further treatment of a patient in accordance with the recognised standards of the relevant medical or other health profession; or

(f) to the giving of information to an official that is relevant to the performance of the official's functions stated in the official's instrument of appointment; or

(g) to the giving of information to the Commonwealth or a State, or an entity of the Commonwealth or a State, by the chief executive if the giving of the information

(i) is determined by the chief executive to be in the public interest; and

(ii) is required to or may be given under an agreement that-

(A) is between Queensland and the Commonwealth, State or entity; and

(B) is prescribed under a regulation for this paragraph; or

(ga) to the giving of information to the chief executive to allow the chief executive to act under paragraph (gb); or

(gb) to the giving of information to another person if the chief executive considers the giving of the information is in the public interest and the information is-

(i) given by the chief executive; or

(ii) given, with the chief executive's written authority, by an officer, employee or agent of the department; or

(h) to the giving of information to another officer, employee or agent of the department if-

(i) the other officer, employee or agent is authorised in writing by the chief executive to receive the information; and

(ii) the giving and receipt of the information is-

(A) to give effect to or manage a funding arrangement; or

(B) to give the information under paragraph (g); or

(i) to the giving of information to a board established under a health practitioner registration Act or the Queensland Nursing Council for the purposes of-

(i) making, or giving information about, a complaint about a person registered under the health practitioner registration Act or the Nursing Act 1992; or

(ii) answering questions or otherwise giving information as part of an investigation or a disciplinary proceeding about a person registered under the health practitioner registration Act or the Nursing Act 1992; or

(j) to the giving of information to a committee declared under section 31(1) to be an approved quality assurance committee, or to a person authorised by the committee to receive the information, to enable the committee to perform its functions.

(3) The Commonwealth, a State or entity that receives information under an agreement under subsection (2)(g)

(a) must not give it to anyone else; and

(b) must ensure the information is used only for the purpose for which it was given under the agreement.

(4) A person who has been an officer, employee or agent of the department or a dissolved authority must not give to any other person, directly or indirectly, any information acquired by reason of being such an officer, employee or agent which, immediately before that person ceased to be such an officer, employee or agent, it was his or her duty not to disclose.

Maximum penalty – 50 penalty units.

(4A) Subsection (4) does not apply if-

(a) the information is given to-

(i) the chief executive; or

(ii) another officer, employee or agent of the department who is authorised in writing by the chief executive to receive the information; and

(b) the purpose of the giving and receipt of the information is to give the information under subsection (2)(gb).

(4B) In the department's annual report for a financial year under the Financial Administration and Audit Act 1977, the chief executive must include details of-

(a) the nature of any information given, under subsection (2)(gb), during the financial year; and

(b) the purpose for which the information was given.

(4C) However, the details mentioned in subsection (4B) must not identify, directly or indirectly, the person to whom the information relates.

(5) This section does not apply to officials.

("Health practitioner registration Act" is defined to include a range of such legislation. "Officials" is defined to mean only auditors and investigators appointed under the Act).

The potential impingement on activities promoted by NHMRC is that health information cannot be disclosed by a Queensland public health sector agency unless it can be done in conformity with this section, as it overrides the NPPs.

Guidelines on collection, use or disclosure for research, statistical purposes or a health service

Appendix 4 of the Information Privacy Guidelines (2003), is entitled:

Guidelines for the collection, use and disclosure of health information required for:

(a) research relevant to public health or public safety; or

(b) the compilation or analysis of statistics relevant to public health or public safety and

(c) guidelines for the collection of health information for the management, funding or monitoring of a health service.

In relation to these guidelines, it is said at page 55:

> "Under IS42A, the Department is required to make or adopt guidelines for NPP2.1(d) and 10.3(d). The following Guidelines have been developed to meet these requirements. Consistency with the Section 95A guidelines has been maintained to the greatest possible extent. Changes have however been necessary to take account of the statutory environment within which Queensland Health operates."

The guidelines that follow are closely based on the section 95A guidelines but written to apply to actions of collection or use or disclosure by officers of the Queensland Department of Health.

SOUTH AUSTRALIA

Confidentiality provisions

Examples include:

(a) section 57 of the *Public Sector Management Act 1995* that makes unauthorised disclosure of information a ground for disciplinary action against a public employee.

(b) section 42 of the *Public and Environmental Health Act 1987* prohibits a person having medical information or information about the personal affairs of a person from intentionally disclosing that information unless in the course of official duties, with the consent of the person or when required by a court order.

Privacy regulation

South Australia has established by Cabinet Administrative Instruction No.1 of 1989 a set of information privacy principles that are applicable to all agencies and instrumentalities in the South Australian public sector.

The principles are based on the IPPs in the Federal Privacy Act. Those relevant to use and disclosure of information held by public sector agencies are set out at pages 3–4:

Use of Personal Information

(7) Personal information should not be used except for a purpose to which it is relevant.

(8) Personal information should not be used by an agency for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose unless:

(a) the record-subject has expressly or impliedly consented to the use;

(b) the agency using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person.

(c) the use is required by or under law; or

(d) the use for that other purpose is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer.

Disclosure of Personal Information

(10) An agency should not disclose personal information about some other person to a third person unless:

(a) the record – subject has expressly or impliedly consented to the disclosure;

(b) the person disclosing the information 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 record – subject or of some other person;

(c) the disclosure is required or authorised by or under law; or

(d) the disclosure is reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty or for the protection of the public revenue or for the protection of the interests of the government, statutory authority or statutory office-holder as an employer.

The limitations on use and disclosure are thus similar to those under the Federal Privacy Act, but there is no explicit provision that would have the same effect as section 95.

However, South Australia has established the Privacy Committee of South Australia by order of the Governor-in-Council of 17 May 2001. Its functions are generally advisory as to the operation of the administrative IPPs but it does have authority to exempt a person or body from one or more of the Information Privacy Principles on such conditions as the Committee thinks fit.

TASMANIA

Confidentiality provisions

Examples include section 139 of the *Public Health Act 1997* that prohibits a person from disclosing information about a person that is on the cervical cytology register unless with consent of the person, to the person's medical practitioner on certain conditions or for the purpose of the Act.

Privacy regulation

The Tasmanian government has adopted a set of privacy principles as an administrative guide to govern the collection, storage, use and disclosure of personal information in the public sector. These are based closely on the IPPs in the Federal Privacy Act.

In relation to activities that NHMRC promotes, there are two important departures from the text of IPPs 10 and 11 that relate to use and disclosure respectively. The text of the relevant paragraphs at pages 6–7 is:

Principle 10

Limits on use of personal information

1.A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

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

(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;

(c) use of the information for that other purpose is required or authorised by or under law;

(d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained; or

(f) the record-keeper considers that the use of the information for that purpose is in the public interest.

Principle 11

Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

(d) the disclosure is required or authorised by or under law;

(e) the disclosure is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue;

(f) the record-keeper considers that the disclosure is in the public interest.

Both principles contain a requirement that a record-keeper who makes a determination under clause 1(f) must:

(a) include in the record a statement of the reasons as to why it has been decided that it is in the public interest to use the information for that purpose; and

(b) if reasonable in the circumstances, notify the person(s) concerned, identifying the nature of the information and its intended use or disclosure.

The addition of sub-paragraph (f) in both principles offers a record keeper a broader discretion to use or disclose personal information than that contained in the IPPs.

Explanatory notes to the Tasmanian principles, at page 12, make it clear that this discretion is to be exercised with caution:

> "It is important to ensure that decisions regarding disclosure in the public interest are not taken in a routine or ad hoc manner, but are individually and seriously considered, preferably by the Head of Agency".
>
> 'It should also be noted that, if an agency decides to use or disclose information on grounds of public interest, then the use or disclosure must be limited to the action which is deemed to be in the public interest".
>
> 'The requirement to notify the individual concerned when information is used or disclosed in the public interest, mirrors provisions of the FOI Act which apply in the case of disclosure of 'information relating to the personal affairs of a person'. In such cases, the agency is required by the Act to consult, where reasonable, with the person concerned, who also has appeal rights under the Act."

VICTORIA

There are two Victorian acts that regulate the handling of personal information in the public sector in Victoria: the *Information Privacy Act 2000* and the *Health Records Act 2001*.

The latter act has been discussed above in its application to the private sector and it applies the same standards, ie compliance with Health Privacy Principles in Schedule One to the Act to public sector agencies.

The Victorian *Information Privacy Act* regulates the collection, storage, use and disclosure of personal information that is not health information. Its relevance to NHMRC is whether it contains restrictions on those matters.

The Information Privacy Act applies Information Privacy Principles to the conduct of Victorian public sector agencies. These principles are not identical to either the IPPs or the NPPs but blend elements of both and, in relevant aspects, appear to be less strict than their Federal counterparts.

Collection

Principle 1 is substantially similar to IPP 1, but Principle 10, relating to collection of sensitive information provides that, generally speaking, such information can only be collected with consent. However, paragraph 10.2 provides:

10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if-

(a) the collection-

(i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational
services; or

(ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and

(b) there is no reasonably practicable alternative to collecting the information for that purpose; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection.

Use and Disclosure

Similarly, the provision permitting use and disclosure for research purposes is no different.

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless-

(a) both of the following apply-

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure;or

(c) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual-

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information;

This appears to allow use of identifiable information for research so long as there is no identifying publication, that it is impracticable to seek consent before use or disclosure and that there is a reasonable belief that there will be no further disclosure.

WESTERN AUSTRALIA

Confidentiality provisions

Examples include:

(a) section 81 of the *Criminal Code 1913* prohibits public servants publishing or communicating facts of which they are aware by virtue of their position and which it is their duty to keep secret.

(b) Regulation 8 of the *Public Service Regulation 1988* prohibits an officer from using for any purpose other than the discharge of duties of office any information gained through employment in the Public Service.

(c) section 314 of the *Health Act 1911* imposes similar secrecy obligations.

Privacy regulation

Western Australia has not enacted privacy legislation nor promulgated any administrative regulations dealing generally with the protection of privacy in the public or private sectors.

Confidentiality of Health Information Committee (CHIC)

This committee has been established within the Department of Health and reviews all research that involves access to any health information held in the public sector.

It is not constituted as an HREC but this is being considered.

PART SIX

THE NATIONAL HEALTH PRIVACY CODE

The proposed Code is an initiative of the Australian Health Ministers Advisory Council and is in draft form at the date of writing. It is available on-line at http://www.health.gov.au/pubs/nhpcode.htm

Scope

The Code is designed to apply to all health service providers in their handling of health information. Relevant definitions are:

"**health information** means:

(a) information or an opinion about:

(i) the physical, mental or psychological health (at any time), of an individual; or

(ii) a disability (at any time) of an individual; or

(iii) an individual's expressed wishes about the future provision of health services to him or her; or

(iv) a health service provided, or to be provided, to an individual – that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(d) genetic information about an individual in a form which is, or could be, predictive (at any time) of the health of the individual or any other individual (including antecedents or descendants) – but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information in accordance with a State or Territory Act";

"**health service** means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual service provider or the organisation performing it-

(i) to assess, maintain or improve the individual's health; or

(ii) to diagnose the individual's illness, injury or disability; or

(iii) to treat the individual's illness, injury or disability or suspected illness, injury or disability; or

(b) a disability service, palliative care service or aged care service; or

(c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist – but does not include a health service, or a class of health service, that is prescribed as an exempt health service or to the extent that it is prescribed as an exempt health service;

"**health service provider"** means an organisation that provides a health service but does not include a health service provider, or a class of health service provider, that is prescribed as an exempt health service provider or to the extent that it is prescribed as an exempt health service provider under a State or Territory Act.

The Code contains an extended section on access to health information as well as 11 National Health Privacy Principles (NHPPs) that address the (now familiar) topics of collection, use and disclosure, data quality, data security and data retention, openness, access and correction, identifiers, anonymity, transborder data flows, transfer or closure for the practice of a health service provider and making health information available to other health service providers.

For comparison purposes, the NHPPs on collection and use and disclosure, NHPPs 1 and 2 are:

NHPP 1. Collection

When health information may be collected

1.1 An organisation must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and at least one of the following applies-

(a) the individual has consented;

(b) the collection is required, authorised or permitted, whether expressly or impliedly, by or under law;

(c) the information is necessary to provide a health service to the individual and the individual is incapable of giving consent and

(i) it is not reasonably practicable to obtain the consent of an authorised representative of the individual; or

(ii) the individual does not have an authorised representative;

(d) the collection is the result of a disclosure made in accordance with NHPP 2.2(a), 2.2(f), 2.2(i), 2.2(j), 2.2(m), 2.4, 2.5 or NHPP 6;

(e) if the collection is necessary for research, or the compilation or analysis of statistics, in the public interest -

(i) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(ii) it is impracticable for the organisation to seek the individual's consent to the collection; and

(iii) the information is collected in accordance with guidelines issued for the purposes of this sub-paragraph;

(f) the collection is necessary to prevent or lessen-

(i) a serious and imminent threat to the life, health, welfare or safety of any individual; or

(ii) a serious threat to public health or public safety and the collection is by or on behalf of a public sector organisation – and the information is collected in accordance with guidelines, if any, issued for the purposes of this paragraph;

(g) the collection is by or on behalf of a law enforcement agency and the organisation reasonably believes that the collection is necessary for a law enforcement function; or

(h) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim; or

(i) the information is a family medical history, social medical history or other relevant information about an individual, that is collected for the purpose of providing a person (including the individual) with a health service, and is collected by a health service provider:

(i) from the person who is to receive that service; or

(ii) from a relative or carer of the individual; or

(iii) in any other situation, in accordance with any guidelines issued for the purposes of this paragraph.

How health information is to be collected

1.2 An organisation must collect health information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 if it is reasonable and practicable to do so, an organisation must collect health information about an individual only from that individual.

1.4 At or before the time (or, if that is not practicable, as soon as practicable thereafter) an organisation collects health information about an individual from the individual, the organisation must take steps that are reasonable in the circumstances to ensure that the individual is aware of-

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.5 If an organisation collects health information about an individual from someone else, it must take steps (if any), that are reasonable in the circumstances to ensure that the individual is or has been made aware of

the matters listed in NHPP 1.4 except to the extent that the information is collected under NHPP 1.1(i), or where making the individual aware of the matters would pose a serious threat to the life or health of any individual.

NHPP 2. Use and Disclosure

2.1 An organisation may use or disclose health information about an individual for the primary purpose for which the information was collected.

2.2 An organisation must not use or disclose health information about an individual for a purpose (the "secondary purpose") other than the primary purpose for which the information was collected unless-

(a) both of the following apply-

(i) the secondary purpose is directly related to the primary purpose; and

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) the use or disclosure is required, authorised or permitted, whether expressly or impliedly, by or under law; or

(d) all of the following apply-

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use or disclosure for the secondary purpose is reasonably necessary for the provision of the health service; and

(iii) the individual is incapable of giving consent; and

(A) it is not reasonably practical to obtain the consent of an authorised representative of the individual; or

(B) the individual does not have an authorised representative; or

(e) all of the following apply-

(i) the organisation is a health service provider providing a health service to the individual; and

(ii) the use is for the purpose of the provision of further health services to the individual by the organisation; and

(iii) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively; and

(iv) the information is used in accordance with guidelines, if any, issued for the purposes of this paragraph; or

(f) the use or disclosure is for the purpose of

(i) funding, management, planning, monitoring, improvement or evaluation of health services; or

(ii) training provided by a health service provider to employees or persons working with or being trained by the organisation; and

(iii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the individual's consent to the use or disclosure; or

(iv) reasonable steps are taken to de-identify the information; and

(v) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication; and

(vi) the information is used or disclosed in accordance with guidelines, if any, issued for the purposes of this paragraph; or

(g) if the use or disclosure is necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(iii) the use or disclosure is conducted in accordance with guidelines issued for the purposes of this paragraph; and

(iv) in the case of disclosure-

(A) the organisation reasonably believes that the recipient of the health information will not disclose the health information; and

(B) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained; or

(h) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent

(i) a serious and imminent threat to an individual's life, health, safety or welfare; or

(ii) a serious threat to public health or public safety; and – the information is used or disclosed in accordance with guidelines, if any, issued for the purposes of this paragraph; or

(i) in the case of genetic information of an individual which is or could be predictive at any time of the health of another individual

(i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to that other individual's life or health; and

(A) reasonable steps have been made to obtain consent of the first mentioned individual; or

(B) it is not reasonably practicable to obtain consent of that individual; or

(C) that individual is incapable of giving consent; and

(iii) the use or disclosure is in accordance with guidelines issued for the purposes of this paragraph; or

(j) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and

(i) uses or discloses the information in reporting its concerns to relevant persons or authorities; and

(ii) if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence;[1] or

(k) the organisation reasonably believes that

(i) the use or disclosure is reasonably necessary for a law enforcement function by or on behalf of a law enforcement agency and,

(ii) if the organisation is a registered health service provider, the use or disclosure would not be a breach of confidence;[2] or

(l) the use or disclosure is necessary for the establishment, exercise or defence of a legal or equitable claim; or

(m) the health information is about a deceased individual and is to be used by, or disclosed to

(i) a legal representative of the deceased individual; or

(ii) a person who was an authorised representative of the deceased individual, and the disclosure is for a purpose related to the former powers, functions or duties of that person; or

(iii) a person nominated in writing by the deceased individual prior to their death as eligible to receive the information; or

(iv) a next of kin of the deceased person; or

(v) any other person in accordance with guidelines, if any, issued for the purposes of this paragraph; and in the case of a disclosure to a next of kin, the organisation has no reasonable grounds to believe that the deceased would have objected to the disclosure to that person.

1. This ensures that a registered health service provider must not disclose information to a law enforcement agency or other body unless satisfied that the disclosure would also be authorised under the general law of confidence – both common law and equity. The general law currently applies to providers and only permits disclosure in rare cases where the duty of confidence is outweighed by a countervailing public interest in law enforcement.

2. This ensures that a registered health service provider must not disclose information to a law enforcement agency or other body unless satisfied that the disclosure would also be authorised under the general law of confidence – both common law and equity. The general law currently applies to providers and only permits disclosure in rare cases where the duty of confidence is outweighed by a countervailing public interest in law enforcement.

Note 1:Nothing in NHPP 2 requires an organisation to disclose health information about an individual. An organisation is always entitled not to disclose health information in the absence of a legal obligation to disclose it.

Note 2:An organisation is also subject to the requirements of NHPP 9 if it transfers personal information to a person in another jurisdiction.

2.3 If an organisation discloses health information under paragraph (j) or (k) of NHPP 2.2, it must make a written note of the disclosure.

2.4 Despite NHPP 2.2, where an individual is incapable of giving consent, there are circumstances under which an organisation providing a health service to the individual may disclose health information about the individual to another person if

(a) the disclosure is to a person responsible for the individual, and, in the opinion of the person who is providing the health service, is necessary for the continued provision of appropriate health services to, or care of, the individual; or

(b) the disclosure is made for compassionate reasons; and

(i) the organisation believes that the disclosure would reasonably be expected by the individual; and

(ii) the disclosure is not contrary to any wishes previously expressed by the individual of which the organisation is reasonably aware or of which the organisation could reasonably be expected to be aware; or

(c) the disclosure is made to the individual's authorised representative in order for the representative to make decisions about the individual's care and treatment or to perform functions or duties related to their powers as an authorised representative.[3]

2.5 Despite NHPP 2.2, an organisation may use or disclose health information about an individual where-

(a) it is known or suspected that the individual is dead; or

(b) it is known or suspected that the individual is missing; or

(c) the individual has been involved in an accident or other misadventure and is incapable of consenting to the use or disclosure – and the use or disclosure is to the extent reasonably necessary

(d) to identify the individual or ascertain their whereabouts; or

(e) to ascertain the identity and location of an immediate family member or other relative or close friend of the individual for the purpose of-

(i) enabling a member of the police force, a coroner or other prescribed organisation to contact the immediate family member, other relative or close friend for compassionate reasons; or

3. This provision does not limit the power of an authorised representative(s) under the general law or this Code to consent to the disclosureof health information to themselves or others.

(ii) to assist in the identification or location of the individual – and, in the circumstances referred to in paragraph (b) or (c)

(f) the use or disclosure is not contrary to any wish-

(i) expressed by the individual before he or she went missing or became incapable of consenting and not withdrawn by the individual; and

(ii) of which the organisation is aware or could have become aware by taking reasonable steps; and

(g) the information is used or disclosed in accordance with guidelines, if any, issued for the purposes of this paragraph.

Implementation of the Code

At the time of writing four alternative implementation strategies are contemplated. These have the potential to affect the handling of health information at both levels in all jurisdictions.

1. The Code would be adopted as a schedule to the *Privacy Act 1988* and the scope extended to cover all health information – ie in the Australian Government public sector, in all State and Territory public sectors and in the private sector. States and Territories would vacate the field of health privacy;

2. The Code would be adopted by or incorporated into State and Territory legislation, and would cover the public and private sectors in each State and Territory. Australian Government legislation would incorporate the Code for the Australian Government public sector. The Australian Government would vacate the private sector;

3. The Code would be adopted as a schedule to the *Privacy Act 1988*, and would cover the Australian Government public sector and the private sector nationally. The Code would also be adopted by or incorporated into State and Territory privacy arrangements (legislative or administrative) and would only cover the State and Territory public sectors;

4. The Code would be adopted as a schedule to the *Privacy Act 1988*, and would continue to cover the Australian Government public sector and the private sector. The Code would also be adopted by or incorporated into State and Territory privacy arrangements (legislative or administrative). States and Territories would have the option of retaining their legislation for the private sector.

PART SEVEN

INTERNATIONAL

THE EUROPEAN PARLIAMENT AND COUNCIL OF EUROPE

The Parliament passed the Directive 95/46/EC on the protection of individuals with regard to processing of personal data and on the free movement of such data on 24 October 1995.

This appears to be the basic privacy directive, although more specific ones have been issued since, relating to the electronic communications sector, processing of personal data by the Community institutions and processing of personal data in the telecommunications sector.

The Directive operates at a broad level of directing member states to implement measures to achieve protection and so contains principles at a very broad level that are not simple to apply to the Australian context. It is available at http://www.europa.eu.int/eur-lex/enl.

Central concepts

The Directive applies a number of prohibitions of the processing of personal data and requires controllers and processors to abide by these. The key definitions in Article 2 are:

'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction:

'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law:

'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

The key relevant obligations are those Articles in SECTION II on Criteria for making Data Processing Legitimate. Article 7 is the general prohibition and provides:

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

More specific protection is applied to what is commonly referred to as sensitive information in Australian law, by Article 8:

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

The remaining Articles focus on access by the data subject to her or his data, the provision of information to data subjects about the identity of the data controller, the purposes of processing the data etc, the data subject's right to object to the processing and national organisational systems to implement the protection.

From this brief account of the Directive, it appears that it offers too general a level of principles to assist in a review of the Australian privacy regulation. For NHMRC's interests, there is only one specific reference to the use of data for research – and

that relates to the exemption from access by data subjects to their data. The issues that are addressed in Australian legislation appear to be covered by far wider provisions authorising processing of data in the public interest.

UNITED STATES OF AMERICA

Under the *Federal Health Insurance and Portability Act 1996,* regulations have been promulgated that took effect in April 2003 that apply a privacy protection regime to personal health information. The regulation is called the HIPAA Privacy Rule and cited as 45 Code of Federal Regulations Parts 160 and 164.

Scope

The rule applies to all covered entities that are health plans, health care clearing house and health care providers who transmit personal health information in connection with transactions, such as billing and payment for services or insurance, in respect of which the Department of Health and Human Service has established standards.

The rule generally prohibits health care providers from using or disclosing individually identifiable health information, called "protected health information" for purposes other than treatment except in defined situations. The first of these is with consent, called authorisation, to which the standards of consent for involvement in research are applied. The second is if the data are de-identified, or are in limited data sets (established by removing specified identifiers). The third is with waiver of authorisation by an institutional review board, applying similar procedures and requirements as apply to the exercise of their power to waive consent for research.

The rule also allows use of protected health information for research purposes if waiver of authorisation (consent) is given by a privacy board, a new body established under the rule.

The regulation is highly detailed, but its key definitions are:

Health information means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and

(ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

NEW ZEALAND

The *Privacy Act 1993* appears to follow a similar pattern to the Australian federal equivalent, in that it is expressed to fulfil New Zealand's obligations as a member of the OECD, but it adopts a simpler comprehensive scheme. Section 46 of the Act permits the Commissioner to approve codes of practice and, in 1995 (amended in 2000), he approved the Health Information Privacy Code, which is directly relevant to the present context. Section 46 permits approved codes to vary or relax the provisions of principles under the Act.

In this account of the legislation, the relevant provisions of this Act and the Code are described and compared.

Scope

The Act

The Act applies to "agencies" that are defined in section 2 to include both public and private sector entities, with specific exclusion of some specific public sector bodies:

"Agency"-

(a) Means any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a Department; but

(b) Does not include-

(i) The Sovereign; or

(ii) The Governor-General or the Administrator of the Government; or

(iii) The House of Representatives; or

(iv) A member of Parliament

(iv) A member of Parliament in his or her official capacity; or

(v) The Parliamentary Service Commission; or

(vi) The Parliamentary Service, except in relation to personal information about any employee or former employee of that agency in his or her capacity as such an employee; or

(vii) In relation to its judicial functions, a court; or

(viii) In relation to its judicial functions, a [tribunal]; or

(ix) An Ombudsman; or

(x) A Royal Commission; or

(xi) A commission of inquiry appointed by an Order in Council made under the Commissions of Inquiry Act 1908; or

(xii) A commission of inquiry or board of inquiry or court of inquiry or committee of inquiry appointed, pursuant to, and not by, any provision of an Act, to inquire into a specified matter; or

(xiii) In relation to its news activities, any news medium.

The Code

The Code, in paragraph 3, adapts the definition of agency to specify:

(a) an agency which provides health or disability services;

(b) within a larger agency, a division or administrative unit (including an individual) which provides health or disability services to employees of the agency or some other limited class of persons;

(c) a person who is approved as a counsellor for the purposes of the *Accident Insurance Act 1998*;

(d) a school, faculty or department of a tertiary educational institution which provides the training or a component of the training necessary for the registration of a health professional;

(e) an agency having statutory responsibility for the registration of any registered health professionals;

(f) a health professional body;

(g) persons appointed or designated under the *Health and Disability Commissioner Act 1994*;

(h) the Health Funding Authority or an agency that has been declared by the Minister of Health by notice in the Gazette to be a funder for the purposes of the *Health and Disability Services Act 1993*;

(i) an agency which provides health, disability, accident or medical insurance, or which provides claims management services in relation to such insurance, but only in respect of providing that insurance or those services;

(j) an accredited employer under the *Accident Insurance Act 1998*;

(k) an agency which provides services in respect of health information, including an agency which provides those services under an agreement with another agency;

(l) a district inspector, deputy district inspector or official visitor appointed pursuant to section 94 of the *Mental Health (Compulsory Assessment and Treatment) Act 1992*;

(m) an agency which manufactures, sells or supplies medicines, medical devices or related products;

(n) an agency which provides health and disability services consumer advocacy services;

(o) the Department for Courts but only in respect of information contained in documents referred to in section 44(2) of the *Coroners Act 1988*;

(p) the agencies specified in Schedule 1.

Personal information

The Act

The Act applies to handling of personal information which has in section 3 a simpler and wider definition than that in Australian legislation:

"**Personal information**" means information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar-General pursuant to the *Births, Deaths, and Marriages Registration Act 1995*, or any former Act:

Health information

The Code

The Code applies to health information that is defined in clause 4(1) as:

(a) information about the health of that individual, including his or her medical history;

(b) information about any disabilities that individual has, or has had;

(c) information about any health services or disability services that are being provided, or have been provided, to that individual;

(d) information provided by that individual in connection with the donation, by that individual, of any body part or any bodily substance of that individual or derived from the testing or examination of any body part, or any bodily substance of that individual; or

(e) information about that individual which is collected before or in the course of, and incidental to, the provision of any health service or disability service to that individual.

The Act contains 12 Information Privacy Principles that address the activities of collection, storage, security, access, use and disclosure, similar to the Australian equivalents.

The Code contains 12 Health Information Privacy Rules that address:

1. Purpose of Collection
2. Source
3. Collection
4. Manner of Collection
5. Storage and Security
6. Access
7. Correction
8. Accuracy
9. Retention
10. Limits on use
11. Limits on Disclosure
12. Unique identifiers

The Principles and the Rules contain less restrictive provisions than the Australian equivalents, as Principle 2 and Rules 2 & 3 on Collection, Principles 10 and 11 and Rules 10 and 11 indicate.

PRINCIPLE 2

Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.

(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,-

- (a) That the information is publicly available information; or
- (b) That the individual concerned authorises collection of the information from someone else; or
- (c) That non-compliance would not prejudice the interests of the individual concerned; or
- (d) That non-compliance is necessary -
  - (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
  - (ii) For the enforcement of a law imposing a pecuniary penalty; or
  - (iii) For the protection of the public revenue; or
  - (iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or
- (e) That compliance would prejudice the purposes of the collection; or
- (f) That compliance is not reasonably practicable in the circumstances of the particular case; or
- (g) That the information -
  - (i) Will not be used in a form in which the individual concerned is identified; or
  - (ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- (h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

The provisions of sub-paragraph (g) are notable in that they permit departure from the requirements of collecting personal information only from the individual concerned if the use of the information will not identify the individual.

The Code Rule 2 provides that collection must be from the person concerned but permits an agency to not comply with this if it believes on reasonable grounds:-

- (a) that the individual concerned authorises collection of the information from someone else having been made aware of the matters set out in subrule 3(1);

(b) that the individual is unable to give his or her authority and the health agency having made the individual's representative aware of the matters set out in subrule 3(1) collects the information from the representative or the representative authorises collection from someone else;

(c) that compliance would:

(i) prejudice the interests of the individual concerned;

(ii) prejudice the purposes of collection; or

(iii) prejudice the safety of any individual;

(d) that compliance is not reasonably practicable in the circumstances of the particular case;

(e) that the collection is for the purpose of assembling a family or genetic history of an individual and is collected directly from that individual;

(f) that the information is publicly available information;

(g) that the information:

(i) will not be used in a form in which the individual concerned is identified;

(ii) will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) will be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned;

(h) that non-compliance is necessary:

(i) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences;

(ii) for the protection of the public revenue; or

(iii) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(i) that the collection is in accordance with an authority granted under section 54 of the Act.

The Code Rule 3 permits an agency to depart from the requirement of notifying a person about information collected from a third party if the agency believes on reasonable grounds:[1]

(b) that compliance would:

(i) prejudice the interests of the individual concerned; or

(ii) prejudice the purposes of collection;

(c) that compliance is not reasonably practicable in the circumstances of the particular case; or

[1] paragraph (a) of this Rule has been revoked.

(d) that non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences.

The Principles and Rules that relate to the use and disclosure of information are:

PRINCIPLE 10

Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds -

(a) That the source of the information is a publicly available publication; or

(b) That the use of the information for that other purpose is authorised by the individual concerned; or

(c) That non-compliance is necessary -

  (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

  (ii) For the enforcement of a law imposing a pecuniary penalty; or

  (iii) For the protection of the public revenue; or

  (iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to-

  (i) Public health or public safety; or

  (ii) The life or health of the individual concerned or another individual; or

(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) That the information -

  (i) Is used in a form in which the individual concerned is not identified; or

  (ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) That the use of the information is in accordance with an authority granted under section 54 of this Act.

The Code Rule 10 on use of health information follows closely the structure and content of Principle 10 in the Act. It prohibits an agency from using health information for a purpose other than that of collection unless it believes certain matters on reasonable grounds. In relation to use for research, the requisite belief is:

(e) that the information:

(i) is used in a form in which the individual concerned is not identified;

(ii) is used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) is used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form that could reasonably be expected to identify the individual concerned;

Principle 11 in the Act and Rule 11 of the Code address disclosure:

PRINCIPLE 11

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds -

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) That the source of the information is a publicly available publication; or

(c) That the disclosure is to the individual concerned; or

(d) That the disclosure is authorised by the individual concerned; or

(e) That non-compliance is necessary -

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or [tribunal] (being proceedings that have been commenced or are reasonably in contemplation); or

(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to -

(i) Public health or public safety; or

(ii) The life or health of the individual concerned or another individual; or

(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) That the information

(i) Is to be used in a form in which the individual concerned is not identified; or

(ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

Rule 11 of the Code on disclosure follows closely the form and substance of Principle 11. Accordingly, it permits disclosure when, among other circumstances, it is authorised by the individual. The Rule then states that compliance with the consent provision is not necessary where an agency believes on reasonable grounds that it is either not desirable or not practicable to obtain authorisation from the individual concerned and one of a number of specified circumstances obtains. The circumstance relevant to disclosure for research (Rule 11 (2) (c)) reads:

that the information:

(i) is to be used in a form in which the individual concerned is not identified;

(ii) is to be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(iii) is to be used for research purposes (for which approval by an ethics committee, if required, has been given) and will not be published in a form which could reasonably be expected to identify the individual concerned;

Ethics committee is defined in clause 3 to mean:

(a) the Ethics Committee of the Health Research Council of New Zealand;

(b) the National Advisory Committee on Health and Disability Services Ethics; or

(c) an ethics committee constituted in accordance with the currently applicable Standard for Ethics Committees promulgated by the Ministry of Health.

The references to a review by an ethics committee "if required" is ambiguous as there is no statutory provision for review so that the requirement is thought to mean an ethical or institutional requirement. The Rules do not provide any additional guidance for an ethics committee. Accordingly, it appears that the committee is not required to do more than review the ethical acceptability of the research.

Summary comment

Under the New Zealand statutory Principles and Code Rules, personal information can be used or disclosed by an agency, without authorisation of the individual, in similar circumstances as under the Australian NPPs. The exceptions for directly related purposes, public law enforcement, revenue protection and prevention of harm in emergencies are similar. However, as with the New Zealand collection principle, the Principles and the Code Rules appear to allow identifying information to be used or disclosed for statistical or research purposes, provided only that the

information is used in a form that does not identify or is not published in a form that could identify an individual. These provisions appear to overcome the difficulty created by the Australian NPPs that prohibit the actual use or disclosure without consent.

The reference to section 54 of the Act is to the power of the Privacy Commissioner to authorise an agency to collect, use or disclose personal information in breach of principles 2, 10 or 11, if the Commissioner is satisfied, in the special circumstances of the case,

> (a) The public interest in that collection or, as the case requires, that use or that disclosure outweighs, to a substantial degree, any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure; or
>
> (b) That collection or, as the case requires, that use or that disclosure involves a clear benefit to the individual concerned that outweighs any interference with the privacy of the individual that could result from that collection or, as the case requires, that use or that disclosure.

(2) The Commissioner may impose in respect of any authority granted under subsection (1) of this section such conditions as the Commissioner thinks fit.

(3) The Commissioner shall not grant an authority under subsection (1) of this section in respect of the collection, use, or disclosure of any personal information for any purpose if the individual concerned has refused to authorise the collection or, as the case requires, the use or disclosure of the information for that purpose.

This appears to be the equivalent to the power given by sections 71–80E of the *Federal Privacy Act 1988* to the Australian Privacy Commissioner to issue a Public Interest Determination.

CANADA

The right to privacy is regarded as part of the rights of Canadian citizens guaranteed by the Charter of Rights and Freedoms that is a schedule to the Canadian Constitution.

There is both federal and provincial legislation on privacy. Federal legislation in Canada comprises two statutes: the *Privacy Act 1980* that applies to federal government institutions and the *Personal Information Protection and Electronic Documents Act 2000* that applies to all organisations in the private sector.

Provincial legislation appears to be substantially uniform and a detailed comparison has been conducted by the Canadian Institutes of Health Research and published as a compendium in 2000. It is understood the Institutes are updating this. The existing compendium is available at http://www.cihr-irsc.gc.ca/e/about/pdf_15561.htm. The Institutes are presently undertaking a number of research initiatives in this area. The preface to the Compendium contains the following explanation of the task and the publication:

"The protection of personal health information is a matter of great concern for most Canadians given its fundamental and intimate connection with the right to dignity, integrity and autonomy. Yet, at the same time, access to such information is indispensable to researchers seeking to improve the health status of Canadians and the viability and sustainability of the health care system as a whole. This dilemma has perplexed legislators for some time and continues to raise even more complex questions, especially in this age of electronic data. Recent years have seen a plethora of privacy legislation emerge across the country. Stakeholders in the health research field are struggling to make sense of this increasing body of laws and regulations, hoping to understand how all of it may or may not ultimately affect them. Some argue that the laws and regulations have gone too far, while others argue, not far enough. All recognize, however, that there is undoubtedly more to come on the horizon and agree on the need to better understand the implications of the emerging legislative and regulatory framework.

Against this backdrop, the Medical Research Council of Canada (as it then was), Standing Committee on Ethics, Sub-Committee on Legislation (the "Sub-Committee") decided to examine this area of law more closely and to seriously reflect on how legislators have fared until now in striking an appropriate balance between the desire to protect the rights of individuals (and collectivities), on the one hand, and the desire to promote the improvement of Canada's health care system and overall health status, on the other. As a first step in its analysis, the Sub-Committee commissioned the editor to prepare this Compendium of Canadian Legislation Respecting the Protection of Personal Information in Health Research.

This working tool was specifically designed to provide members of the Sub-Committee with a panoramic view of the legislative landscape across the country. Organized by theme and by jurisdiction, the compendium allows for comparisons to be drawn and certain trends to be deduced. Cross-links between relevant sections of various laws and regulations have been parenthetically noted for easy reference. This compendium is intended to serve as a springboard for organizing future discussion, developing common terminology and clarifying issues in the current privacy debate. Other stakeholders in the health research field may hopefully find this compendium useful as a means of surveying, at least in a preliminary fashion, the applicable law on various aspects of privacy and data protection in any given jurisdiction."

The preface to the definition provisions (p.3.0) offers a useful overview of Canadian provincial approaches:

> "In this section, we have divided relevant legislation into two general categories. The first category of statutes pertains to the protection of personal information in general. These statutes define
>
> "personal information" by enumerating a wide range of different types of information, including basic health information such as, an individual's fingerprints, blood type or inheritable characteristics, medical history or health and health care history. All of these statutes provide that such personal information may be recorded in virtually any form.
>
> The second category of statutes pertains more specifically to the protection of personal health information. These statutes specifically define "personal health information" in some detail. Such definitions include information about: the individual's physical or mental health; any health services provided to the individual; any donation by the individual of a body part or bodily substance and any information derived from an examination of that body part or bodily substance; any sale or dispensing of a drug, device or equipment pursuant to a prescription; as well as any other information that is collected in the course of providing health services to the individual or incidentally to the provision of such services. Also included in most definitions of personal health information is registration information, such as, an individual's personal health number, his or her health service eligibility information and any payment or billing information.
>
> These statutes likewise provide that personal health information may be recorded in virtually any form. Interestingly, Alberta's Health Information Act (Bill 40) expressly protects the confidentiality of non-recorded personal health information (sections 29 and 44 infra). Alberta's Health Information Act (Bill 40) is, to date, the only statute that expressly incorporates, within its definition of personal health information, detailed information relating directly to health service providers, including their personal, business and professional data. It is also worth noting a recent tendency by legislators to expressly define terms such as "non-identifying health information" and "de-identified personal health information". As will become apparent in later sections, this tendency reflects a growing recognition that, given technological advances, personal health information can vary along a spectrum of identifiability and corresponding degree of risk, thereby warranting distinct legal treatment in each case."

The prefaces to the sections containing provisions on collection (p.4.0) and on use and disclosure (p.5.0) are also useful for the same reason:

Collection:

In general, collection of personal (health) information must relate directly to an operating program or activity of a public institution, or to an identified and/or authorized purpose of the person or organization collecting the information. In some cases, the purpose or object of the file must be documented. The collection must be by fair and lawful means and must be limited to that which is reasonably necessary

to accomplish the purpose for which the personal information is being collected. Interestingly, Bill C–6 further subjects the collection to an overriding "reasonable person" standard, requiring that collection be limited to only those purposes that a reasonable person would consider appropriate in the circumstances. The collection must be made, wherever possible, directly from the individual to whom it relates. The individual must be informed of the legal authority for collecting personal information, the purpose for which it is being collected and, in some cases, its anticipated use and/or disclosure. Exceptionally, personal (health) information may be collected from someone other than the individual the information is about, with or without the latter's knowledge or consent. Such exceptions include situations where:

- collection from the individual directly is likely to result in inaccurate information, to defeat the purpose for which the information is being collected or to prejudice the health or safety of the individual or that of others;
- collection from the individual directly is not reasonably practicable;
- the personal (health) information is otherwise publicly available;
- collection is clearly in the interests of the individual, yet time and circumstances do not allow for the individual to be contacted directly;
- personal (health) information is elsewhere in the same Act permitted to be disclosed for a certain purpose, and the Act expressly includes a correlative permission to collect such information for the same purpose (eg. for research);
- collection is authorized by law or regulations.

In both the Alberta and Saskatchewan Health Information Acts, personal health information may be collected from a person other than the subject of the information where the purpose is to assemble a family (or genetic) history. Whereas Alberta's statute limits this latter exception to the health care context, Saskatchewan's statute does not so specify. It is interesting to note that in some of the statutes pertaining specifically to the protection of personal health information, separate rules exist for the collection of personal health numbers (eg. Alberta, Saskatchewan, Manitoba). Also noteworthy is an increasing tendency to subject the collection of personal health information to a "need-to-know" test. A case in point is Alberta's Health Information Act (Bill 40) that actually sets up a hierarchy of permissible collection. A custodian must first consider whether the collection of aggregate health information would be adequate for the intended purpose and, if so, must limit collection to that. If aggregate health information is not considered adequate for the intended purpose, the custodian must then consider whether other non-identifying health information would be adequate and, if so, must limit collection accordingly. Only if other non-identifying health information is still not adequate for the intended purpose, can the custodian then collect identifying personal health information in accordance with the Act.

Use and disclosure:

In principle, personal (health) information can only be used and/or disclosed for the purpose for which it was collected or for a purpose consistent therewith. What

constitutes a consistent purpose is usually defined in the statute in question. Any other proposed use or disclosure generally requires the consent of the individual the personal (health) information is about.

Notwithstanding this general principle, personal (health) information may be used and/or disclosed for a research purpose without the consent of the individual the information is about in certain limited conditions prescribed by law or regulation. As will become readily apparent, these conditions vary significantly in terms of stringency, complexity and level of detail. For instance, these may range from the simple requirement of a bona fide or legitimate research purpose to more extensive conditions including any combination or variation of the following:

- the use/disclosure is limited to the extent necessary to carry out the described purpose;
- the purpose cannot reasonably be accomplished unless the information is in identifiable form;
- any record linkage is not harmful and the benefits of the record linkage are clearly in the public or societal interest;
- the purpose justifies the action proposed;
- the intended use/disclosure is not frivolous and the ends contemplated cannot be achieved unless the information is communicated in nominative form (Quebec);
- it is unreasonable, impractical or unfeasible to obtain consent;
- the purpose has been approved by the Privacy Commissioner (eg. Quebec) or the Privacy Commissioner has at least been informed thereof (Federal Bill C–6);
- the intended use/disclosure has been reviewed and/or approved by a research ethics committee (eg. Alberta) or some other designated review committee (eg. Manitoba);
- the researcher will not subsequently use and/or disclose identifiable information for another purpose without prior authorization;
- the researcher will not publish research findings in a form that would allow the subject of the information to be readily identified;
- the researcher will remove and/or destroy all identifying information at the earliest opportunity;
- the researcher is qualified to carry out the research (Alberta);
- the researcher will not contact the subject of the information directly, unless the original custodian of the information has first obtained the subject's consent to be contacted by the researcher;
- the researcher will take reasonable steps to ensure the security and confidentiality of the personal (health) information;

- the researcher has made a written undertaking, or has signed a research agreement with the original custodian of the personal (health) information, promising to comply with these and other conditions required by law. (In some cases, the specific content of such an agreement is set out in the Act itself or in accompanying regulations, eg. Alberta, Saskatchewan, Ontario. Interestingly, Alberta's Health Information Act also includes detailed provisions setting out available recourses in the event of breach of the agreement).

Typically, the above conditions will not apply to information that has been in existence for more than 100 years or if the person the information is about has been dead for over 25 years. As mentioned above (see section on "Collection"), the provision which allows a custodian to disclose personal (health) information for a research purpose, is typically accompanied by a correlative provision which allows the researcher in question to collect the information for that same purpose.

Privacy Act 1980

Scope

The Act applies to all government institutions that are listed in a schedule to the Act.

It applies to the collection and handling by those institutions of personal information, which is defined in simple and comprehensive terms in section 3:

"personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e) but excluding

the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

  (i) the fact that the individual is or was an officer or employee of the government institution,

  (ii) the title, business address and telephone number of the individual,

  (iii) the classification, salary range and responsibilities of the position held by the individual,

  (iv) the name of the individual on a document prepared by the individual in the course of employment, and

  (v) the personal opinions or views of the individual given in the course of employment,

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years;

The exclusion of certain information for the purposes of sections 7, 8 & 26 (which impose limits on use and disclosure by a government institution) and section 19 of the Access to Information Act (which imposes limits on access) operate to make free from such limits information about public sector employees, contractors or licensees and people deceased for more than 20 years.

Collection

Sections 4–6 of the Act prohibit a government institution from collecting personal information unless it relates directly to "an operating program or activity of the institution." Collection is to be from the individual wherever possible, unless the individual authorises otherwise or where disclosure is permitted by another institution. Individuals must be informed of the purpose of the collection. However, the requirements for direct collection and notification of purpose do not apply if they may result in the collection of inaccurate information or would defeat the purpose or prejudice the use for which the information collected.

Use and disclosure

Section 7 provides that a government institution may use information for the purpose for which it was collected, for a use "consistent with that purpose" or for a use for which the information may be disclosed.

Disclosure

Section 8 permits institutions to disclose information for the following range of purposes:

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

(d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

(e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

(f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;

(h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;

(i) to the National Archives of Canada for archival purposes;

(j) to any person or body for research or statistical purposes if the head of the government institution

  (i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and

(ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;

(k) to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;

(l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

Paragraphs (j)(i) and j(ii) and m(i) and m(ii) show that use and disclosure of personal information by a federal government institution is less regulated than in Australia. It is the government institution, rather than an HREC as in Australia, that determines that the purpose cannot be achieved by using de-identified information and who obtains an undertaking from the researcher or body to whom the information is disclosed that it will not disclose the information in a way that identifies a person.

Paragraph (m) is a very broad ranging power that also relies on the government institution determining the public interest balance and the individual benefit.

Personal Information Protection and Electronic Documents Act 2000

Scope

This Act applies to every organisation, defined as "includes an association, a partnership, a person and a trade union."

It imposes on organisations obligations to conform to principles contained in a Schedule to the Act. There are ten principles that deal with:

Accountability

Identifying purposes

Consent

Limiting Collection,

Limiting Use, Disclosure and Retention

Accuracy

Safeguards

Openness

Individual Access

Challenging Compliance.

These principles need to be read in conjunction with sections 5 to 10, namely "protection of personal information" of the Personal Information Protection and Electronic Documents Act.

Collection

Principles 2 and 4 address the relevant issues.

4.2 Principle 2 – Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1 The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2 Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfil these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6 This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.4 **Principle 4 – Limiting Collection**

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1 Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.

Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2 The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3 This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

These paragraphs plainly depend on the consent and the use and disclosure principles. These are as follows, again in full, not only to show their clarity but because the effect of sections 5–10 cannot be readily understood otherwise.

4.3 **Principle 3 – Consent**

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2 The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3 An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4 The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6 The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7 Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

4.3.8 An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.5 Principle 5 – Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

4.5.1 Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2 Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4 This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

In the absence of any other provisions, these principles confine the use or disclosure of personal information to the purposes for which it was collected or for other purpose so long as the individual has given consent in accordance with Principle 3. However, it is that Principle whose application is varied by other sections.

In particular section 7 varies the consent requirement in relation to collection, use and disclosure. In relation to collection, section 7(1) provides:

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

(c) the collection is solely for journalistic, artistic or literary purposes; or

(d) the information is publicly available and is specified by the regulations.

Of more relevance for comparison to Australia, subsections (2), (3), (4) and (5) vary the application of Principles 3 (on consent) and 5 (on use and disclosure). Only subsections (2) and (3) are reproduced as these contain the substantive provisions:

Use without knowledge or consent

(2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if

(a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;

(b) it is used for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual;

(c) it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used;

(c.1) it is publicly available and is specified by the regulations; or

(d) it was collected under paragraph (1)(a) or (b).

Disclosure without knowledge or consent

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

(a) made to, in the Province of Quebec, an advocate or notary or, in any other province, a barrister or solicitor who is representing the organization;

(b) for the purpose of collecting a debt owed by the individual to the organization;

(c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

(c.2) made to the government institution mentioned in section 7 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act as required by that section;

(c.2)* made to the government institution mentioned in section 7 of the Proceeds of Crime (Money Laundering) Act as required by that section;

*[Note: Paragraph 7(3)(c.2), as enacted by paragraph 97(1)(a) of chapter 17 of the Statutes of Canada, 2000, will be repealed at a later date.]

(d) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

(f) for statistical, or scholarly study or research, purposes that cannot be achieved without disclosing the information, it is impracticable to obtain consent and the organization informs the Commissioner of the disclosure before the information is disclosed;

(g) made to an institution whose functions include the conservation of records of historic or archival importance, and the disclosure is made for the purpose of such conservation;

(h) made after the earlier of

(i) one hundred years after the record containing the information was created, and

(ii) twenty years after the death of the individual whom the information is about;

(h.1) of information that is publicly available and is specified by the regulations;

(h.2) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or

(i) required by law.

The effect of these provisions is to relax the operation of the use and disclosure principles to permit use or disclosure without consent for research purposes where the purposes cannot be achieved otherwise, obtaining consent is impracticable and the organisation informs the Privacy Commissioner of the use or disclosure.