NSW HEALTH DEPARTMENT

CIRCULAR

	File No	99/9945
	Circular No	2000/62
	Issued	26 July 2000
	Contact	Ms J Kelly (02) 9391 9110 Information Management and Clinical Systems Branch

NSW HEALTH PRIVACY MANAGEMENT PLAN

The *Privacy and Personal Information Protection Act 1998*

The *Privacy and Personal Information Protection Act* commenced on 1 July 2000. The Act provides for the protection of personal information and for the protection of the privacy of individuals generally. The Act establishes privacy principles that must be observed by public sector agencies.

Health Privacy Management Plan

Section 33 of the Act requires each public sector agency to prepare and implement a privacy management plan. The Health Privacy Management Plan has been prepared to meet these requirements.

The Plan consists of two documents:

- Privacy Protection Guidelines, which identify how all NSW Health agencies will comply with the Information Privacy Protection Principles in the *Privacy and Personal Information Protection Act*
- Internal Review Guidelines, which provide procedures for the review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the Act.

Scope

The Health Privacy Management Plan applies to all NSW Health agencies. This includes all public health organisations under the Health Services Act 1997, the NSW Department of Health, and the Ambulance Service.

Information Privacy Policy

NSW Health has already established an information privacy policy for health information, which was distributed as the Information Privacy Code of Practice (IPCOP), Circular No 99/18. While the IPCOP predates the Act, it is NSW Health's major policy document on information privacy and is designed to ensure that personal health information is collected, stored and used in accordance with information privacy protection principles. **Circular 99/18 continues to apply to all NSW health agencies.**

Distributed in accordance with circular list(s):

A		**B**		**C**	58	**D**		**E**									
F	10	**G**		**H**	20	**I**		**J**	42								
K		**L**		**M**		**N**		**P**		**Q**							

73 Miller Street North Sydney NSW 2060
Locked Mail Bag 961 North Sydney NSW 2059
Telephone (02) 9391 9000 Facsimile (02) 9391 9101

Health Privacy Code of Practice
The Act allows the Attorney General, at the request of an agency, to make a privacy code of practice, which can exclude the agency from the operation of one or more information protection principles in the Act, or modify the way the information protection principles apply to the agency.

The Health Privacy Code of Practice has been made under section 29 of the Act to modify the application of the information protection principles. The Health Privacy Code of Practice applies to all public health organisations under the Health Services Act, the NSW Department of Health, and the Ambulance Service. A copy is included in the Plan.

CONSULTATION
The Health Privacy Management Plan has been developed in consultation with Area Health Services and other affiliated organisations, and endorsed by the NSW Health Information Privacy Steering Committee. Comments on the Plan should be forwarded to Joanna Kelly, Associate Director, Health Informatics (jkely@doh.health.nsw.gov.au).

Michael Reid
DIRECTOR GENERAL

PRIVACY MANAGEMENT PLAN

PART 1: PRIVACY PROTECTION GUIDELINES

PART 2: INTERNAL REVIEW GUIDELINES

PART 1: PRIVACY PROTECTION GUIDELINES

Table of Contents

INTRODUCTION

The Privacy Protection Guidelines identify how all NSW Health agencies will comply with the Information Privacy Protection Principles in the *NSW Privacy and Personal Information Protection Act 1998*.

These guidelines have been developed in accordance with sections 33 (2) (a) and (b) of the Act, and form part of the NSW Health privacy management plan.

The existing NSW Health Information Privacy Code of Practice (IPCOP), Circular No 99/18, continues to apply to all NSW Health agencies. Where there is any doubt in applying these guidelines, reference should be made to the IPCOP.

1 THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998

1.1 The Privacy and Personal Information Protection Act

The *Privacy and Personal Information Protection (PPIP) Act 1998* provides for the protection of personal information, and for the protection of the privacy of individuals generally. The Act establishes privacy principles that must be observed by all public sector agencies. These principles are based on the OECD Guidelines on the Protection of Privacy and Flows of Transborder Data adopted in 1981.

Section 33 of the Act requires each NSW public sector agency to make a privacy management plan setting out how it will comply with the Act. The Act also allows the Attorney General, at the request of an agency, to make a privacy code of practice which can exclude the agency from the operation of one or more information protection principles, or modify the way the information protection principles apply to the agency.

See Appendix D for the Health Privacy Code of Practice made under section 29 of the Act.

The Privacy Commissioner may also make privacy codes of practice which may apply to public sector agencies. The Privacy Code of Practice for Research, the Privacy Code of Practice for Investigations, and the Privacy Code of Practice for Inter-agency Transfers of Information will apply to NSW Health when they take effect.

1.2 Application of the Act to the public health system

The Act applies to all NSW Health agencies. This includes

- all public health organisations under the *Health Services Act 1997*
- the NSW Department of Health, established under the *Health Administration Act 1982*

- the Ambulance Service of NSW, established under the *Ambulance Service Act 1990*.

The term "NSW Health" is used in these guidelines as a broad description covering all these agencies.

1.3 The Information Protection Principles

The information protection principles[1] are set out in Part 2 of the Act. They establish standards for collecting and dealing with personal information so as to minimise the risk of misuse of that information. The principles also allow individuals to exercise a reasonable degree of control over what happens to their own personal information.

The privacy principles pay as much attention to matters such as the collection (four principles) and storage of information (four principles) as they do to its use (two principles) and disclosure (two principles).

Under section 21 of the Act, agencies are required to comply with the principles, and any breach of the principles will give a person an automatic right to seek an internal review[2] from the agency responsible for the breach.

1.4 Information Privacy Policy

NSW Health has already established an information privacy policy for health information, which was distributed as the Information Privacy Code of Practice (IPCOP), Circular No 99/18.

While the IPCOP predates the Act, it is NSW Health's major policy document on information privacy and is designed to ensure that personal health information is collected, stored and used in accordance with information privacy protection principles.

The IPCOP remains in force. A new edition of the IPCOP will be updated with reference to the PPIP Act and the Health Privacy Code, and will be re-released as the Information Privacy Policy.

2 DEFINITIONS

2.1 Personal Information

The Act defines personal information as "information or an opinion (including information or an opinion forming part of a data base 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". Personal information includes such things as an individual's fingerprints, retina prints, body samples, genetic characteristics, video recordings, photographs and electronic records. The person's identity does not have to be expressly indicated by the information, it is only necessary that it "can reasonably be ascertained from the information".

[1] *Privacy NSW* A Guide to the Information Protection Principles
[2] *NSW Health* Internal Review Guidelines

The Act excludes certain types of information from the definition. The most significant exceptions are:

- information contained in a publicly available publication
- information about an individual's suitability for public sector employment
- information about people who have been dead for more than 30 years
- a number of exceptions relating to law enforcement investigations.

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

Personal information held by NSW Health agencies

Personal information is held by an agency when it is:

- in possession or control of the information, or
- the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement, or
- the information is contained in a State record in respect of which the agency is responsible under the State Records Act 1998

Personal information is not collected by a NSW Health agency if the receipt of the information by the agency is unsolicited. However, the use, storage and access provisions of the PPIP Act will apply to such information in so far as it is personal information.

2.3 Sensitive Information

The degree of sensitivity of the personal information may influence the way in which the information protection principles are applied[3]. Many of the principles only require that "reasonable" steps be taken having regard to all the circumstances. The more sensitive the nature of the information, the higher the level of care should be used by staff when dealing with the information, particularly where disclosure to a third party is being considered.

Although all personal health information should be considered sensitive, the client/patient may indicate that their information regarding a particular condition or treatment is particularly sensitive. Examples of highly sensitive information include sexual assault, genetic testing.

2.4 Privacy and confidentiality

Confidentiality is an obligation which restricts an agency from using or disclosing any information in a way which is contrary to the interests of the person or organisation which provided it in the first place. Confidentiality can be defined as a mode of managing private information, by the restriction of access to information to authorised persons, entities and processes at authorised times, in an authorised manner (see Appendix F concerning confidentiality obligations under law).

Privacy applies only to personal information and applies irrespective of who provided it to the agency. Privacy is a broader concept than confidentiality and relates to an

[3] *Privacy NSW* A Guide to the Information Protection Principles

individual's ability to control the extent to which their personal information, enabling identification, is available to others.

2.5 Use and disclosure of personal information

The information protection principles distinguish between use and disclosure[4]. Use refers to the treatment and handling of personal information within an organisation, particularly when this involves making decisions on the basis of the information. Disclosure refers to making personal information available to people outside the organisation, other than to the individual concerned and includes the publication of personal information.

2.6 Public registers

Under the PPIP Act, a public register is a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee). The Act regulates the way in which government agencies must deal with public registers, and the Information Protection Principles apply to the personal information held in public registers[5].

Information on public registers should only be made available for legitimate purposes, that is a purpose relating to the purpose of the register or of the Act under which the register is kept. Certain people have the right to have personal details on a public register suppressed, that is, where the agency is satisfied that the safety or well-being of a person will be affected by not suppressing the information, and where the agency is satisfied that the suppression is not against the public interest.

The provisions of section 57 - disclosure of personal information contained in public registers, are not required to be complied with in respect of the registers of registered health practitioners (see clause 8 of the Health Privacy Code, Appendix D).

[4] *Privacy NSW* A Guide to the Information Protection Principles
[5] *Privacy NSW* A Guide to Public Registers

3 INFORMATION PROTECTION PRINCIPLES

3.1 Section 8 – Collection for lawful purposes (principle 1)

(1) A public sector agency must not collect personal information unless:
- *(a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and*
- *(b) the collection of the information is reasonably necessary for that purpose*

(2) A public sector agency must not collect personal information by any unlawful means.

Explanation
This principle limits the amount of personal information collected by reference to the function and purposes of the agency.

Issues for Compliance
The functions of NSW Health are established primarily under the *Health Services Act 1997,* and the *Health Administration Act 1982.*

Examples of purposes for which personal health information is collected include:
- service delivery, or
- continuity of care, or
- clinical productivity, or decision making, or
- protection of public health, or
- research, or
- quality measurement or management, or
- funding and payment.

3.2 Section 9 – Collection of personal information directly from the individual (principle 2)

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:
- *(a) the individual has authorised collection of the information from someone else, or*
- *(b) in the case of information relating to a person who is under the age of 16 years – the information has been provided by a parent or guardian of the person.*

Issue for Compliance
Where the information is acquired from a private or non-government agency, arrangements will need to be made for the individuals concerned to authorise its transfer to the public sector agency.

Exemptions to section 9

1. Under the Act

- if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal (section 23(2))
- where a public sector agency is investigating or otherwise handling a complaint which could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency (section 24(4))
- with lawful authorisation or permission not to comply (section 25)
- if compliance by the agency would, in the circumstances, prejudice the interests of the individual to whom the information relates (section 26(1))
- Collection from other agencies[6] : Where a disclosure by a public sector agency A to another public sector agency B, is a lawful disclosure by A under the *Privacy and Personal Information Protection Act*, for example, between Area Health Services, then the receipt of the information by agency B is legitimate, and the collection from a source other than the individual concerned is unaffected by section 9.

2. Under a Code

- Consent to disclose information by person other than the person to whom the information relates (Health Privacy Code clause 7)
  (a) A public sector agency listed in clause 2(a) of the Code may disclose information with the consent of the person responsible where:
    (i) the person to whom the information relates is deceased or physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure; and
    (ii) the disclosure is not contrary to any wish (of which the agency is aware) expressed by the person to whom the information relates before that person became unable to give or communicate consent.
  (b) In subclause (a), *person responsible* has the same meaning as in section 33A of the Guardianship Act 1987.

3.3 Section 10 – Requirements when collecting personal information (principle 3)

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:

(a) the fact that the information is being collected
(b) the purposes for which the information is being collected
(c) the intended recipients of the information
(d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided
(e) the existence of any right of access to, and correction of, the information

[6] *Privacy NSW* A Guide to the Information Protection Principles

(f) the name and address of the agency that is collecting the information and the agency that is to hold the information.

Explanation
This principle aims to ensure that when people are asked to provide their personal information to a public sector agency, they are given enough information in order to exercise any rights that they may have under the Act.

Issues for Compliance
When personal information is collected from an individual, the obligation is to provide information in broad terms about the collection, including the recipients of the information and purposes for which the information will be used. (Further information on informing individuals is available in section 9 of the discussion paper Ethical Management of Health Information, and will be incorporated in the Information Privacy Policy).

In most cases these requirements can be met by including the necessary information on the application form used to collect personal information, or where information is collected over a counter, by an appropriately displayed sign. When information is collected over the phone and people are asked to identify themselves, or are capable of being automatically identified, an appropriate verbal notice should be prepared or a written notice sent by way of acknowledgement of the call.

A sample privacy information sheet meeting section 10 requirements, and designed for use at the time of collection, is attached at Appendix A. Agencies may develop privacy information sheets in consultation with the Department of Health.

Exemptions to section 10
1. Under the Act
Section 10 does not apply to information collected:
- where a public sector agency is investigating or otherwise handling a complaint which could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency (section 24(4))
- with lawful authorisation or permission not to comply (section 25)
- if compliance by the agency would, in the circumstances, prejudice the interests of the individual to whom the information relates (section 26(1))
- if the individual to whom the information relates has expressly consented to the agency not complying with the principle (section 26(2)).

3.4 Section 11 – Other requirements relating to collection of personal information (principle 4)

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete, and

(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

Explanation
Agencies must take reasonable steps to ensure that the personal information they collect from an individual is accurate, and that the way it is collected does not unreasonably intrude on the personal affairs of the individual to whom it relates.

Issues for Compliance
What is reasonable to satisfy the requirement that the information is relevant, not excessive, accurate, up to date and complete will vary from case to case, and will involve a balancing of various factors[7] such as:

- the purpose for which the information was collected
- the sensitivity of the information
- how many people will have access to the information
- the importance of accuracy to the proposed use
- the potential effects for the individual concerned if the information is inaccurate, out-of-date or irrelevant
- the opportunities to subsequently correct the data
- the ease with which agencies can check the data.

The second part of this principle aims to prevent the use of unreasonable methods or techniques to gather personal information, for example video surveillance. Again, what is reasonable will vary from case to case.

Standard quality management procedures will be followed by NSW Health agencies to ensure the accuracy of information.

3.5 Section 12 – Retention and security of personal information (principle 5)

A public sector agency that holds personal information must ensure:

(a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and

[7] *Privacy NSW* A Guide to the Information Protection Principles

(c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

Explanation
This principle sets out standards for the storage of personal information once it has been collected.

Part (d) places an obligation on agencies which transfer personal information to outside parties to ensure that this information is not used or disclosed inappropriately. It will generally apply where an agency transfers personal information to an outside person or organisation for the performance of a service to the agency, including consultants, information technology service providers, and external providers of human resources and financial services.

Issues for Compliance
Policies and procedures for management of information and records will be followed by all NSW Health agencies[8].

NSW Health agencies will comply with the provisions of the *State Records Act 1998,* which covers retention, storage and disposal of state records.

NSW Health agencies will apply the following measures with respect to security safeguards[9]:

- data will be kept in safe custody, sufficient to prevent unauthorised access
- the data will be properly handled and preserved to prevent loss or deterioration or unauthorised destruction
- where transmission of data is required, all reasonable measures will be taken to ensure its safety, integrity and confidentiality.

The level and type of security will depend respectively, on the sensitivity of the personal information and the medium in which it is stored.

In relation to section 12(d), where it is necessary for personal information to be transferred to any third party for the purpose of providing the agency with a service, the agency will seek wherever possible, to obtain from that party a Confidentiality undertaking to prevent unauthorised use or disclosure of that information, and to indemnify NSW Health against any breaches of the Act, Code or the undertaking (see Appendix E).

[8] *NSW Health* Records Management Procedure Manual
[9] Privacy Code of Practice for the NSW public sector Workforce Profile - 1999

3.6 Section 13 – Information about personal information held by agencies (principle 6)

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

- *(a) whether the agency holds personal information, and*
- *(b) whether the agency holds personal information relating to that person, and*
- *(c) if the agency holds personal information relating to that person:*
  - *(i) the nature of that information, and*
  - *(ii) the main purposes for which the information is used, and*
  - *(iii) that person's entitlement to gain access to the information.*

Explanation
This principle is designed to allow people to ascertain whether an agency holds personal information, and if so, whether the agency holds personal information relating to them.

The PPIP Act also provides that section 13 should be read as if the provisions of the *Freedom Of Information (FOI) Act 1989* apply, meaning agencies are entitled to rely on any conditions or limitations imposed (on access or other matters) under that Act.

Issues for Compliance
All NSW Health agencies should continue to comply with the IPCOP, regarding access by the client/patient to health records.

This principle requires only that an agency takes steps that are reasonable in the circumstances to enable people to find out if personal information is held. What is reasonable in the circumstances[10] will depend on a number of factors including:

- the damaging nature of the information
- the credibility of the information
- the method of storing the information, and
- any other future consequences that the information may have.

Individuals can ascertain the nature, source and main purposes for use of personal information held by NSW Health agencies, by obtaining a copy of the document *Classes of Personal Information*. This document is part of the NSW Health Privacy Management Plan. Each NSW Health agency will have copies of the *Classes of Personal Information* booklet.

NSW Health agencies will take reasonable steps in the circumstances to enable individuals who have submitted a written request to ascertain whether personal information is held about them. An application for information can only be made by the person to whom the personal information relates. Guidelines on access to health records by the client/patient are provided in the IPCOP, and may also be applied to individuals seeking access to their personal information, which is not health related.

[10] *Privacy NSW* A Guide to the Information Protection Principles

NSW Health reserves the right to request an individual to make a FOI application (refer to 3.7).

Exemption to section 13

1. Under the Act

- with lawful authorisation or permission not to comply (section 25).

3.7 Section 14 – Access to personal information held by agencies (principle 7)

A public sector agency that holds personal information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

Explanation

This principle allows people a right of access to their personal information which may be held by public sector agencies.

The PPIP Act also provides that section 14 should be read as if the provisions of the FOI Act apply, meaning agencies are entitled to rely on any conditions or limitations imposed (on access or other matters) under that Act. These conditions and limitations should not be applied rigidly to stop people having access to information about themselves.

Issues for Compliance

As a matter of policy, individuals are guaranteed a right of access to information about them held by public health organisations. They also have a right to access their records under the *Freedom of Information Act*, as well as under the *Privacy and Personal Information Protection Act*.

Agencies should develop guidelines on access to personal information, including application forms. All NSW Health agencies should continue to comply with the IPCOP, regarding access by the client/patient to health records. Charges for access to health records by clients/patients under the IPCOP should be in compliance with Circular 99/68 – Charges for Health Records and Medical Reports.

Agencies may request an individual to make a Freedom of Information application. Cases[11] where FOI procedures for access would be more appropriate will be where the structure provided by the FOI Act will assist the agency in managing a difficult or complex case, for example, cases which are:

- resource intensive, or
- complex, or

[11] *Privacy NSW* A Guide to the Information Protection Principles

- where information is sought as part of a dispute between family members as to whether records should be released, or
- where the request for information may impact on other persons, or identify another person, or
- where there is a clear public interest against access.

The following conditions will apply to access requested under section 14 of the PPIP Act:

- an application for information can only be made by the person to whom the personal information relates
- access to relevant personal information will be provided as soon as possible, and should usually be within 35 days of the date of request
- applications for access will be dealt with by the FOI Officer, or the designated Health Information Manager
- charges for applications and processing of applications should be in compliance with Circular 99/68 – Charges for Health Records and Medical Reports
- verification of the identity of individuals seeking access to their personal information will be in accordance with FOI identification procedures
- forms of access to personal information will correspond to those provided under the FOI Act

Access to staff records will be handled in accordance with Part 5-4.7 of the Public Sector Personnel Handbook.

Exemption to section 14

1. Under the Act

- with lawful authorisation or permission not to comply (section 25).

3.8 Section 15 – Alteration to personal information (principle 8)

(1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information:

(a) is accurate, and

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

(2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

Explanation
This principle provides a right to either amend or to attach a statement to personal information which a person believes to be incorrect or inappropriate. In some cases, this principle will now allow an agency to delete information from their records system, despite requirements of the *State Records Act 1998* to the contrary (section 20(4)).

The *Privacy and Personal Information Protection Act 1998* sets up an alternative method of amending personal information held by public sector agencies to that which operates under the *Freedom of Information Act 1989.* However, the Act does not provide any procedural requirements in relation to this. The PPIP Act also provides that section 14 should be read as if the provisions of the FOI Act apply, meaning agencies are entitled to rely on any conditions or limitations imposed (on access or other matters) under that Act.

Issues for Compliance
As a matter of policy, amendments to records will be done by an addendum to the record. Alterations or deletions should not be made. Procedures for health records are provided in the IPCOP.

NSW Health agencies should develop guidelines on amendment of personal information which will specify circumstances in which simplified amendment principles can be followed, and the circumstances when the Freedom of Information procedures will be used.

Generally, amendments can be made under existing policy (ie IPCOP), or under the PPIP Act, and will be applied[12] if the application relates to a minor amendment (for example, the update of an address), and amendment is timely and its accuracy can be verified. Cases where Freedom of Information procedures for amendment will apply, will generally concern applications for a significant or substantial amendment of a record of a permanent or semi-permanent nature, where the information is available for use by the agency in connection with its administrative functions (section 39 of the FOI Act).

NSW Health agencies will apply the following conditions to amendment of personal information under section 15 of the PPIP Act:
- an application for amendment can only be made by the person to whom the personal information relates
- applications for amendment will be dealt with by the FOI Officer or the designated Health Information Manager
- the application must be in writing and should provide appropriate evidence to satisfy the FOI Officer or the designated Health Information Manager that the proposed amendment is in fact correct and appropriate
- an application to amend relevant personal information will be dealt with within 21 days of the date of application

[12] *Privacy NSW* A Guide to the Information Protection Principles

- verification of the identity of individuals seeking amendment of their personal information will be in accordance with FOI identification procedures
- any amendment to personal information will be done by way of an attachment to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought
- if personal information is amended under section 15 of the PPIP Act, the individual to whom the information relates, is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by NSW Health.

Factors[13] to be taken into account in deciding whether it is reasonably practicable to have recipients of information notified of amendments made under section 15 of the PPIP Act include:

- the purpose for which the information was collected
- who the recipients are
- the sensitivity of the information
- the number of people who will have access to the information
- the importance of accuracy of the information
- the potential effects to the individual if the information is inaccurate, out-of-date or irrelevant
- the ease of notifying recipients
- the cost of notifying recipients.

Exemptions to section 15

1. Under the Act

- with lawful authorisation or permission not to comply (section 25)

3.9 Section 16 – Agency must check accuracy of personal information before use (principle 9)

A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

Explanation

This principle places an obligation on agencies to try to ensure that all personal information used by them is relevant and accurate.

Issues of Compliance

NSW Health agencies should take reasonable steps to check information before use. Factors[14] that should be taken into account include:

- the purpose for which the information was collected
- the sensitivity of the information

[13] *Privacy NSW* A Guide to the Information Protection Principles
[14] *Privacy NSW* A Guide to the Information Protection Principles

- the number of people who will have access to the information
- the importance of accuracy or relevance of the information
- the potential effects for the individual concerned if the information is inaccurate, out-of-date or irrelevant
- any opportunities to correct inaccuracies before the information is used
- the difficulty in checking the information
- the cost involved in checking the information.

Note: where an agency relies on information collected by other agencies to make decisions, this principle would require that adequate standards for information exchange are introduced to ensure that the data is uniformly defined and securely and unambiguously transmitted, so that it means the same thing in both agencies.

3.10 Section 17 – Limits on use of personal information (principle 10)

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.

Explanation
This principle generally restricts use of personal information to the purpose for which the information was collected unless consent is obtained for other uses. Refer also to 3.1 for information about purposes for which information is collected, and 3.3 for information on requirements for informing individuals when collecting information.

Issues for Compliance
Where use of personal information is authorised for a purpose other than that for which the information was collected, consent will be obtained in writing, where possible, and signed by the subject of the personal information. Evidence of informed consent may also be provided in the form of contemporaneous notes. See Appendix B for issues concerning consent.

Exemptions to section 17
1. Under the Act

- to public sector agencies where the use is reasonably necessary for law enforcement purposes or for the protection of public revenue (section 23(4))
- to any public sector agency which is investigating or otherwise handling a complaint which could be referred or made to an investigative agency (section 24(4)
- with lawful authorisation or permission not to comply (section 25)

- to any use which relates to a disclosure to another agency administered by the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier (section 28(3)).

2. Under a Code

- Use for the purposes of legal representation (Health Privacy Code, clause 5)
  A health public sector agency is not required to comply with section 17, 18 or 19 if the information is provided to a person or used for the purposes of:
  (a) complying with any risk management scheme operated by the agency; or
  (b) obtaining legal advice or representation.

3.11 Section 18 – Limits on disclosure of personal information (principle 11)

(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.

(2) If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

Explanation

This principle makes a general rule that personal information should be disclosed only for purposes directly related to the purposes for which the information was collected, subject to the exceptions contained within the principle, and elsewhere in the Act or a Code. Refer to 3.1 for information about purposes for which information is collected. Staff can continue to rely on the provisions of the IPCOP to assist them in determining when disclosure will be lawful.

Issues for Compliance

It is advisable to expressly notify clients at the time of collection if any disclosures are to take place. It cannot be readily assumed that individuals are automatically aware of processes which only indirectly touch on their everyday experience.

Note: Disclosure of personal health information for the purposes of continued care will be in accordance with section 28(2), and Health Privacy Code, clause 3 (see 3.12).

Exemptions to section 18

1. Under the Act

- where the disclosure is made in connection with proceedings for an offence or for law enforcement purposes (section 23(5)(a))
- where the disclosure is to a law enforcement agency to locate a person who has been reported as missing to the police (section 23(5)(b))
- where the disclosure is authorised by a subpoena, search warrant or statutory instrument (section 23(5)(c))
- where the disclosure is reasonably necessary for the protection of the public revenue (section 23(5) (d)(i))
- where the disclosure is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe an offence has been committed (section 23(5)(d)(ii))
- to any public sector agency which is investigating or otherwise handling a complaint which could be referred or made to an investigative agency (section 24(4)
- with lawful authorisation or permission not to comply (section 25)
- where the individual expressly consents (section 26(2))
- to any use which relates to a disclosure to another agency administered by the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier (section 28(3)).

2. Under a Code

- Disclosure for purposes of legal representation (Health Privacy Code clause 5)
  A health public sector agency is not required to comply with section 17, 18 or 19 if the information is provided to a person or used for the purposes of:
  (c) complying with any risk management scheme operated by the agency; or
  (d) obtaining legal advice or representation.

3.12 Section 19 – Special restrictions on disclosure of personal information (principle 12)

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.

(2) A public sector agency that holds personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales unless:

(a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, or
(b) the disclosure is permitted under a privacy code of practice.

(3) For the purposes of subsection (2), a "relevant privacy law" means a law that is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned.

(4) The Privacy Commissioner is, within the year following the commencement of this section, to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales

(5) Subsection (2) does not apply
(a) until after the first anniversary of the commencement of this section, or
(b) until a code referred to in subsection (4) is made,
whichever is the latter.

Explanation
The first part of this principle deals with a number of identified categories of personal information which are subject to more stringent disclosure requirements than that which applies to other kinds of personal information under section 18.

The second part of this principle places restrictions on disclosures of personal information to persons or bodies outside New South Wales. The Privacy Commissioner will develop a Code to deal with issues raised in this section.

Issues for compliance
Circumstances where consent for disclosure of health related information should be obtained, will vary, and will be a matter for professional judgement. Factors which may be taken into account in deciding whether it is reasonably practicable to obtain consent include:
- who the recipients of the information are
- the capacity to verify the identity of the recipients of the information
- the sensitivity of the information
- the number of people who will have access to the information
- the potential effects to the individual
- the urgency with which the information is required
- the capacity to inform the person and seek their consent.

Exemptions to section 19
1. Under the Act
- where the disclosure is reasonably necessary in order to investigate an offence where there are reasonable grounds to believe an offence has been committed or may be committed (section 23(7))
- with lawful authorisation or permission not to comply (section 25)
- where the individual expressly consents (section 26(2))
- to any use which relates to a disclosure to another agency administered by the same Minister for the purpose of informing the Minister about a matter under that administration, or to a disclosure to an agency administered by the Premier for the purpose of informing the Premier (section 28(3)).

- Disclosure of information for the purposes of care or treatment
  A public sector agency is not required to comply with section 19 if, in the case of health related information and in circumstances where the consent of the individual to whom the information relates cannot reasonably be obtained, the disclosure is made by an authorised person to another authorised person involved in the care or treatment of the individual. An authorised person is a medical practitioner, health worker, or other official or employee providing health or community services, who is employed or engaged by a public sector agency (section 28(2)).

  2. Under a Code
  A health public sector agency is not required to comply with section 19 of the Act, if, in the case of health related information and in circumstances where the consent of the individual to whom the information relates cannot reasonably be obtained, the information is provided to a health service provider for the purposes of ensuring the continued care of the individual to whom the information relates (Health Privacy Code clause 3).

- Student Placements (Health Privacy Code clause 4)
  A health public sector agency is not required to comply with section 19, if, in the case of health related information, the information is provided to a person during a placement in the public sector agency undertaken as part of fulfilling the requirements for a tertiary qualification in a health or health related field.

  In such cases, the agency should take steps to ensure that students fill out a Confidentiality Undertaking, as set out in Appendix E.

- Disclosure for the purposes of legal representation (Health Privacy Code clause 5)
  A health public sector agency is not required to comply with section 17, 18 or 19 if the information is provided to a person or used for the purposes of:
  (a) complying with any risk management scheme operated by the agency; or
  (b) obtaining legal advice or representation.

- Disclosure of Information to closest relatives (Health Privacy Code clause 6)
  (a) A health public sector agency [listed] is not required to comply with section 19 if, in the case of health related information, the disclosure is made to an immediate family member and is necessary to provide appropriate care of treatment or is made for compassionate reasons.
  (b) The exemption in clause (a) only applies where:
    (i) the person to whom the information relates is deceased or physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure; and
    (ii) the disclosure is not contrary to any wish (of which the agency is aware) expressed by the person to whom the information relates before that person became unable to give or communicate consent.
  (c) Any disclosure pursuant to this clause must be limited to the extent reasonable and necessary for the purposes of subclause (a).
  (d) In this clause “immediate family member” means, in respect of the person to whom the information relates:

(i) a parent, child or sibling;
(ii) a spouse or defacto spouse;
(iii) a member of the person's household;
(iv) a person with responsibilities as a carer, as defined under section 49S of the Anti Discrimination Act 1977, or;
(v) another person nominated to the public sector agency by the person.

- Consent to disclose information by person other than the person to whom the information relates (Health Privacy Code clause 7)
  (b) A public sector agency listed in clause 2(a) of the Code may disclose information with the consent of the person responsible where:
  (i) the person to whom the information relates is deceased or physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure; and
  (ii) the disclosure is not contrary to any wish (of which the agency is aware) expressed by the person to whom the information relates before that person became unable to give or communicate consent.
  (c) In subclause (a), "person responsible" has the same meaning as in section 33A of the Guardianship Act 1987.

APPENDIX A:
PRIVACY INFORMATION SHEET FOR PERSONAL HEALTH INFORMATION

NSW Health proposes to collect, or has collected, personal health information from you, for purposes including:

- service delivery
- continuity of care
- clinical productivity, or decision making
- protection of public health
- quality measurement, or management
- funding and payment
- research.

This information is personal information for the purposes of the *Privacy and Personal Information Protection Act 1998.*

Health care providers who are treating you, including those employed under contract such as Visiting Medical Officers, and health workers involved in the management of the health system, will have access to your personal health information. If you provide your health service with the name of your GP, a discharge summary will be sent to your GP for continued care.

Although all personal health information is regarded as sensitive, you may indicate that your information regarding a particular condition or treatment is particularly sensitive, and that this information should be placed under restricted access.

The supply of your health information is voluntary, except where authorised under legislation. However, health care providers have an obligation to record details of services provided. Where you decide to withhold or restrict access to your health information, you should be aware that this may compromise your future care or treatment, should further care or treatment be required, particularly where the information is directly related to the required subsequent care or treatment.

Under some Acts including the *Health Administration Act,* and the *Public Health Act,* the Department of Health is required to collect certain information on clients/patients receiving treatment in the public health system. Other authorities are legally entitled to certain information about matters such as Medicare eligibility, the registering of births and deaths, circumstances of death, drink-driving and notifiable diseases (including cancer).

Any person who has access to health information is bound by a duty of confidentiality. The privacy and confidentiality of the personal information held about you will be respected.

You are entitled to see information held about you by NSW Health. You have the right to correct and amend personal information held about you.

Further information about privacy protection is available in the NSW Health Privacy Management Plan at http://xxxxxxxxxxxxxxxxx.

(*Name of health service*) is to be regarded as the principal agency that is to hold this information.

Name and address of health service collecting the information

PRIVACY INFORMATION SHEET FOR PERSONAL INFORMATION

NSW Health proposes to collect, or has collected, personal information from you for purposes including

- the efficient and effective management of the health system, or
- planning, monitoring and evaluation, or
- decision making, or
- quality measurement or management, or
- funding and payment.

The information is personal information for the purposes of the *Privacy and Personal Information Protection Act 1998.*

The intended recipients of the information are officers within NSW Health and other government agencies as authorised.

The supply of this personal information is voluntary, except where authorised under legislation. If you do not wish to supply the requested information, then the processing of your personal affairs may be restricted.

You are entitled to see information held about you by NSW Health. You have the right to correct and amend personal information held about you.

The privacy and confidentiality of the personal information held about you will be respected.

Further information on privacy protection is available in the NSW Health Privacy Management Plan at http://xxxxxxxxxxxxxxxxxxxx.

(*Name of health service*) is to be regarded as the principal agency that is to hold this information.

Name and address of health service collecting the information

APPENDIX B:

CONSENT

The *Privacy and Personal Information Protection Act 1998* provides a number of exemptions to the Information Protection Principles where the person to whom the information relates, or from whom it is being collected, consents to the variation.

Consent can excuse the agency from collecting information directly from the individual to whom it relates, informing the individual of a range of issues under section 10, using the information for a purpose other than for which it was collected, or disclosing the information.

Given the range of matters consent can be given on, the varying types of information, and the different circumstances which may arise, it is not appropriate to rely on a pro forma consent form. In seeking consent, however, agencies should have regard to the following issues:

- permission to disclose personal information can be sought separately, or in the context of obtaining informed consent to medical treatment. In relation to the requirements for obtaining consent to medical treatment, see NSW Health Department Circular 99/16;
- the person should be fully informed of the reason why their consent is requested;
- the person should be fully informed of the purpose of the use or disclosure, (if applicable);
- the person should be notified of the nature of the information to be collected, used, or disclosed (as applicable);
- the person should be notified who the information is to be disclosed to (if applicable);
- the person should be fully informed how the information will be used;
- if permission is sought in the context of treatment at a hospital, and relates to the issuing of a discharge summary, obtain the name of the persons current GP to ensure the summary is sent to the appropriate medical practitioner;
- an opportunity should be provided for the person to seek clarification of any issue arising.

APPENDIX C: OFFENCES UNDER THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998

Corrupt disclosure and use of personal information by public sector officials (section 62)

A public sector official must not, otherwise than in connection with the lawful exercise of his or her official functions, intentionally disclose or use any personal information about another person to which the official has or had access in the exercise of his or her official functions.

Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

A person must not induce or attempt to induce a public sector official (by way of a bribe or other similar corrupt conduct) to disclose any personal information about another person to which the official has or had access in the exercise of his or her official functions.

Maximum penalty: 100 penalty units or imprisonment, or both.

The above two paragraphs do not prohibit a public sector official from disclosing any personal information about another person if the disclosure is made in accordance with the *Protected Disclosures Act 1994*.

Offering to supply personal information that has been disclosed unlawfully (section 63)

A person who offers to supply (whether to a particular person or otherwise), or holds himself or herself out as being able to supply (whether to a particular person or otherwise), personal information that the person knows, or ought reasonably to know, has been or is proposed to be disclosed in contravention of section 62 is guilty of an offence.

Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

Offences relating to dealings with Privacy Commissioner (section 68)

A person must not:

(a) without lawful excuse, wilfully obstruct, hinder or resist the Privacy Commissioner or a member of the staff of the Privacy Commissioner in the exercise of functions under this or any other Act, or
(b) without lawful excuse, refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner under this or any other Act, or
(c) wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner or a member of the staff of the Privacy Commissioner in the exercise of functions under this or any other Act.

Maximum penalty: 10 penalty units.

APPENDIX D:

HEALTH PRIVACY CODE MADE UNDER SECTION 29 of the PRIVACY AND PERSONAL INFORMATION PROTECTION ACT 1998

PART 1 - PRELIMINARY

1. Definitions

(a) In this Code the following words have the following meaning:

(i) "the Act" means the Privacy and Personal Information Protection Act 1998;

(ii) "health public sector agency" means an agency listed in clause 2(a) of the Code

(iii) "register of registered health practitioners" means
A register established pursuant to section 17(1) of the Chiropractors and Osteopaths Act 1991;
The Register of Dental Technicians of New South Wales established pursuant to section 14 of the Dental Technicians Act 1975;
A register established pursuant to section 12 of the Dentists Act 1989;
The Register of Medical Practitioners established pursuant to clause 21 of Schedule 1 to the Medical Practice Act 1992;
The Register of Nurses established pursuant to section 16 of the Nurses Act 1991;
The Register of Optical Dispensers established pursuant to section 21 of the Optical Dispensers Act 1963;
A register established pursuant to section 11 of the Optometrists Act 1930;
The Register of Pharmacists established pursuant to section 12 of the Pharmacy Act 1964;
The Register of Physiotherapists for New South Wales established pursuant to section 20 of the Physiotherapists Registration Act 1945;
A register established pursuant to section 9 of the Podiatrists Act 1989;
A register established pursuant to section 9 of the Psychologists Act 1989.

2. Application (section 29(5))

(a) This Code applies to the following public sector agencies, those being:

(i) a public health organisation, as defined under section 7 of the Health Services Act 1997

(ii) the Ambulance Service of NSW, established pursuant to the Ambulance Services Act 1990

(iii) the NSW Department of Health, a government department established pursuant to section 6 of the Health Administration Act 1982.

(b) This Code applies to:
  (i) any personal information collected, held, and used by agencies listed at 2(a);
  (ii) all activities of the agencies listed at 2(a).

PART 2 – MODIFICATION OF INFORMATION PROTECTION PRINCIPLES

3. Disclosure of information for the purposes of care or treatment

A health public sector agency is not required to comply with section 19 of the Act if, in the case of health related information and in circumstances where the consent of the individual to whom the information relates cannot reasonably be obtained, the information is provided to a health service provider for the purposes of ensuring the continued care of the individual to whom the information relates.

4. Student Placements

A health public sector agency is not required to comply with section 19 if, in the case of health related information, the information is provided to a person during a placement in the public sector agency undertaken as part of fulfilling the requirements for a tertiary qualification in a health or health related field.

5. Use or Disclosure of Information for the purposes of legal representation

A health public sector agency is not required to comply with sections 17, 18 or 19 if the information is provided to a person or used for the purposes of:
  (a) complying with any risk management scheme operated by the agency; or
  (b) obtaining legal advice or representation.

6. Disclosure of Information to closest relatives

(a) A health public sector agency listed is not required to comply with section 19 if, in the case of health related information, the disclosure is made to an immediate family member and is necessary to provide appropriate care or treatment or is made for compassionate reasons.

(b) The exemption in clause 6(a) only applies where:
  (i) the person to whom the information relates is deceased or physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure; and
  (ii) the disclosure is not contrary to any wish (of which the agency is aware) expressed by the person to whom the information relates before that person became unable to give or communicate consent.

(c) Any disclosure pursuant to this clause must be limited to the extent reasonable and necessary for the purposes of subclause 6(a).

(d) In this clause "immediate family member" means, in respect of the person to whom the information relates:
- (i) a parent, child or sibling;
- (ii) a spouse or defacto spouse;
- (iii) a member of the person's household;
- (iv) a person with responsibilities as a carer, as defined under section 49S of the Anti Discrimination Act 1977; or
- (v) another person nominated to the public sector agency by the person.

7. Consent to disclose information by person other than the person to whom the information relates

(a) A public sector agency listed in clause 2(a) of this Code may disclose information with the consent of the person responsible where:
- (i) the person to whom the information relates is deceased or physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure; and
- (ii) the disclosure is not contrary to any wish (of which the agency is aware) expressed by the person to whom the information relates before that person became unable to give or communicate consent.

(b) In subclause 7(a), "person responsible" has the same meaning as in section 33A of the Guardianship Act 1987.

3.1.1.1

8. Public Registers

The provisions of section 57(1) are not required to be complied with in respect of the following public registers:
- registers of registered health professionals.

APPENDIX E:

CONFIDENTIALITY UNDERTAKING

I, (name) …….. understand that, while I am working at (*insert name of agency*), I may have access to personal information collected for purposes of client/patient care or for administrative, statistical or other purposes. I understand that this information is subject to the provisions of the Privacy and Personal Information Protection Act.

I undertake not to knowingly access any personal information unless such information is essential for me to properly and efficiently perform my duties or fulfil my role at (*insert name of agency*). I undertake strictly to preserve the confidentiality of this information and I understand that a breach of this undertaking may, if I am an employee result in disciplinary action. I acknowledge my statutory duty under section 22 of the Health Administration Act 1982 (attached), in relation to the disclosure of information and under the terms of the Privacy and Personal Information Protection Act. In order to fulfil this undertaking, I will not divulge any identifying, personal or health information regarding individual persons, except as authorised by (*insert the name of agency*) or in compliance with relevant legislation.

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

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

Signed …….. in the presence of

(name) ……..

(signature) …….

(position) ……..

Date ……

APPENDIX F:

HEALTH LEGISLATION REQUIRING CONFIDENTIALITY

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

3.1.2 Health Administration Act 1982

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

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

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

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

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

Information covered by clause 13 and which identifies an individual, may only be released by the Director-General, complying with the requirements set out in clause 13(3).

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

3.1.3 Mental Health Act 1990

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

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

3.1.4 Public Health Act 1991

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

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

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

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

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

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

3.1.5 Obligations of health professionals

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

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

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

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

3.1.6 Health service codes of conduct

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

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

PART 2: INTERNAL REVIEW GUIDELINES

Table of Contents

INTRODUCTION

Under section 53 of the *Privacy and Personal Information Protection (PPIP) Act,* individuals have the right to seek a review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the PPIP Act. This right does not apply to conduct which occurred before July 2000.

The request for review can only be made where it is alleged that the agency has:

- breached any of the information protection principles that apply to the agency
- breached any code made under the Act applying to the agency
- disclosed personal information kept in a public register.

The review shall be undertaken in accordance with the procedures set out in these guidelines.

All complaints, inquiries about information privacy, and requests for review, should be treated as serious matters. Individuals who have made an application for internal review may apply to the Administrative Decisions Tribunal (ADT) if they are not satisfied with either the findings of the review, or the action taken by the agency in relation to their application for review. The ADT can make orders, including the imposition of fines up to $40,000.

The *Internal Review Guidelines* form part of the NSW Health Privacy Management Plan. These Guidelines will be released as a circular, applicable to the Department of Health, the public health system and the NSW Ambulance Service.

1 BACKGROUND

1.6 When do these guidelines apply?

Where a person makes an application for a review under section 53, the Act establishes certain legislative requirements for how and when the application can be made, and how it should be dealt with. This document is designed to provide detailed guidelines in respect of these obligations.

Sometimes however, a person may raise some general concerns as to how personal information is being handled, and not specify to the agency that they are requesting a review under the Act. In such cases, agencies should seek to address the person's concerns by reference to existing policies and complaints handling guidelines. For example, a patient may request to have the details of his or her address revised, to ensure the record is accurate. This can readily be done without referral to the internal review processes under the Act. Sometimes however, the person's concerns may not be able to be resolved through these mechanisms. In such cases, an agency may provide the person with details of their rights to an internal review under the Act, and the requirements for lodging an application for review. If the person chooses to exercise these rights, the terms of these guidelines will again apply.

1.2 The process for internal review

Internal review is a process whereby the agency will handle complaints about how it has dealt with personal information. The process will be handled within the agency's existing procedures for Complaints Handling[1].

The process for internal review forms part of NSW Health's privacy management plan. These guidelines:

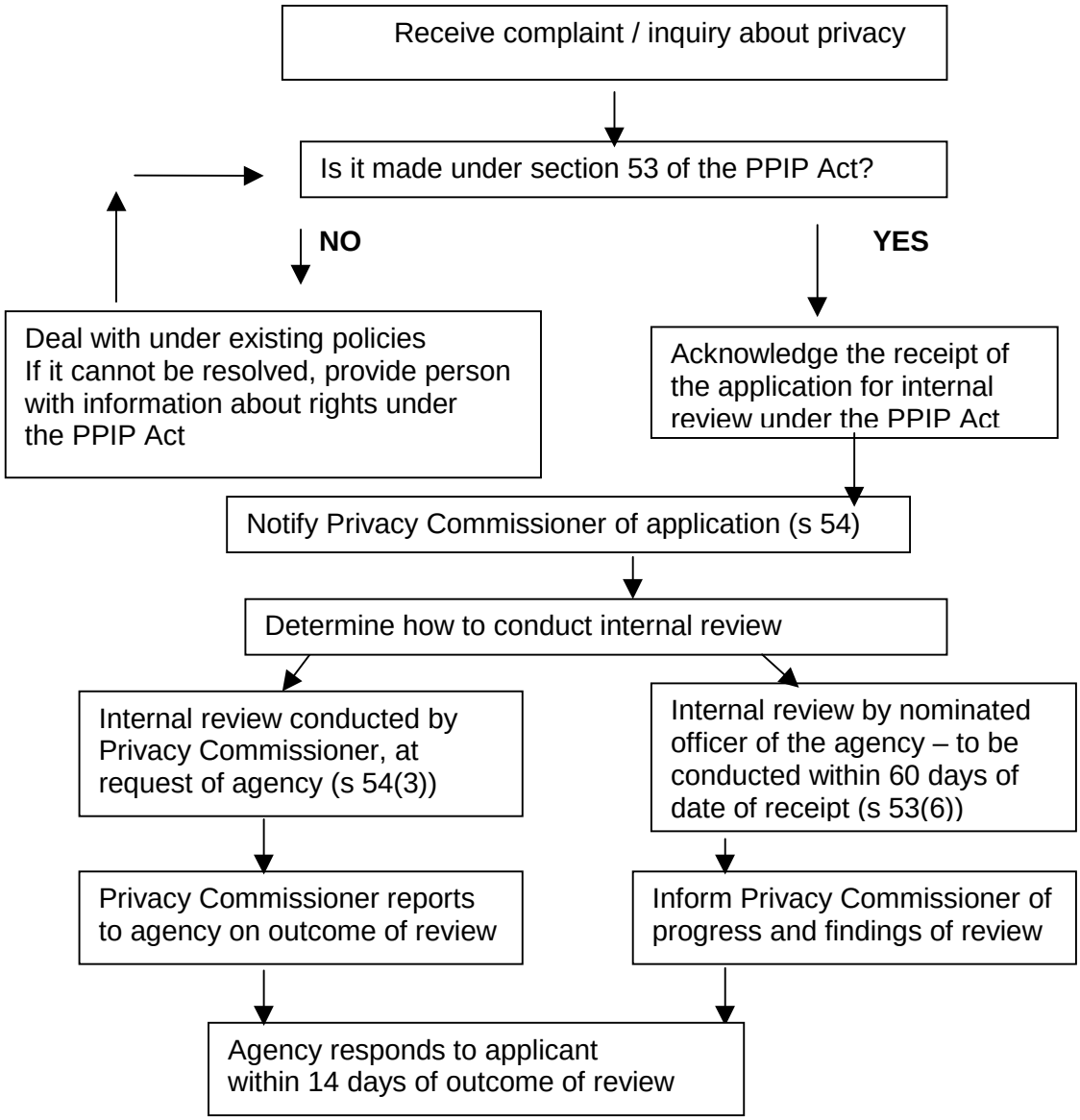
- specify how individuals are informed about their rights to internal review and to seek a review by the ADT
- attach application forms for an internal review under the Act
- indicate who will process applications, and how this will be done, including time limits
- set requirements for recording applications and outcomes
- explain the role of the Privacy Commissioner in the internal review process.

It is important that as part of the Complaints Handling process, a record is kept of the progress of applications for review at each stage of the review process. The record of the internal review will be required by the Department if an application goes to the ADT.

[1] *NSW Health* Better Practice Guidelines for Frontline Complaints Handling

1.3 Complaints handling and the process of internal review

Below is a diagram describing a typical complaints handling process, where the complaint concerns an alleged privacy breach or is a request for an internal review[2].



[2] *NSW Health* Statewide Complaints Data Collection

2 INTERNAL REVIEW PROCESS

2.1 Information about internal review

NSW Health has an obligation to inform individuals of their right to request an internal review, and of their right to seek a review by the ADT. This information and information about the formal requirements for requesting an internal review, shall be made available to health consumers and staff members in brochures and posters (see Appendix 1 for information sheet on internal review).

2.2 The application

The application for internal review can be submitted by anyone who is "aggrieved" by the conduct of the agency. A review can also be sought where the action taken by the agency might only affect the personal information of other individuals[3].

An application for an internal review must, under section 53 (3):

- be in writing, and
- be addressed to the agency
- specify an address in Australia to which the applicant is to be notified after the completion of the Review
- be lodged at an office of the agency within six months from the time the applicant first became aware of the conduct sought to be reviewed.

See Appendix 2 for the form to be used by individuals.

2.3 Privacy Contact Officer

The Department of Health, the NSW Ambulance Service, Area Health Services, affiliated health organisations and statutory health organisations are all required to nominate a person to act as the Privacy Contact Officer for that organisation.

The Privacy Contact Officer should be a senior executive of the organisation, and must have a working knowledge of the Privacy Act.

The Privacy Contact Officer shall be responsible for ensuring the agency meets its obligations under the Act, including keeping the Privacy Commissioner informed of the progress of internal reviews, and of the action proposed to be taken by the agency in relation to the matter. These notifications must be in writing.

The Privacy Contact Officer must keep statistical details about the number of internal review requests received. These statistics will be included in the organisation's annual report, in compliance with section 33(3) of the Act.

2.4 Determining whether the Privacy and Personal Information Protection Act has been breached

The Office of the Privacy Commissioner advises that prior to conducting an internal review, the agency must be satisfied that the complaint or application meets the criteria for an internal review.

[3] *Privacy NSW* A Guide to Internal Reviews

When a complaint or internal review application concerning a privacy matter is lodged, then this must be sent to the Privacy Contact Officer immediately after acknowledgement. The Privacy Contact Officer is required to notify the Privacy Commissioner of all applications for internal review as soon as practicable after receiving the application.

The Privacy Contact Officer will decide whether the matter concerns a breach of an information privacy principle, a code or a public register provision.

If the Privacy Contact Officer is satisfied that the complaint does not involve a clear application under the Act, then an internal review will not be necessary. The complaint should be handled as part of the usual policies for Complaints Handling, with a notification required to the Privacy Commissioner of action proposed to be taken in relation to the matter.

Where internal review is required, then the application will be forwarded by the Privacy Contact Officer to an appropriate Reviewing Officer.

See Appendix 3 for the form to be completed by the Privacy Contact Officer.

2.5 The Reviewing Officer

A Reviewing Officer is any person within the agency who is directed by the Privacy Contact Officer to deal with the application under the terms of the PPIP Act. The Reviewing Officer must be, as far as is practicable, a person who:

- was not substantially involved in any matter relating to the conduct which is the subject of the application
- is an employee or officer of the agency
- is otherwise suitably qualified to deal with the matters raised by the application.

A person may be considered substantially involved in a matter where they have direct or indirect knowledge of the matter whether within or without the relevant agency in which the complaint is made or lodged.

2.6 The Internal Review

2.6.1 The Conduct of the Review

Upon receipt by the Reviewing Officer of an application, the Reviewing Officer must consider any relevant material submitted by the applicant, and by the Privacy Commissioner.

The Reviewing Officer should where practicable, give an opportunity to the applicant to provide written submissions in relation to the matter. The applicant is entitled to have the services of an interpreter.

The Reviewing Officer must complete the review as soon as is reasonably practicable within the circumstances, and in any event, within 60 days from the day on which the application was received. If the review is not completed within 60 days from the day on which the application was received, the applicant is entitled to make

an application to the Administrative Decisions Tribunal for a review of the conduct concerned.

For advice on appropriate conduct of an internal review, refer to the Health Care Complaints Commission's Investigations Manual or the ICAC Procedures Manual.

2.6.2 Completion of the review

The review must recommend any one or more of the following:

- take no further action on the matter
- make a formal apology to the applicant
- take such remedial action as it thinks appropriate (for example, the payment of monetary compensation to the applicant)
- provide undertakings that the conduct will not occur again
- implement administrative measure to ensure that the conduct will not occur again.

The Reviewing Officer shall make recommendations upon completion of the review to the Privacy Contact Officer.

2.6.3 Notification of the applicant

Within 14 days of the completion of the review, the Privacy Contact Officer must notify the applicant in writing of:

- the findings of the review (and the reasons for those findings), and
- the action proposed to be taken by the agency (and the reasons for taking that action), and
- the right of the person to have those findings and the agency's proposed action reviewed by the Administrative Decisions Tribunal.

3 THE ROLE OF THE PRIVACY COMMISSIONER

3.1 Monitoring progress

The Privacy Commissioner has a monitoring role during the course of an internal review. When an application for internal review is received under section 53 of the PPIP Act, all NSW Health agencies will:

- notify the Privacy Commissioner of the application as soon as practicable, and
- keep the Privacy Commissioner informed of the progress of the internal review, and
- inform the Privacy Commissioner of the findings of the review and of the action proposed to be taken by the agency in relation to the matter.

3.2 Complaints relating to privacy

Under section 45 of the PPIP Act, a complaint may be made to the Privacy Commissioner about the alleged violation of, or interference with, the privacy of an individual. The subject matter of a complaint may relate to conduct to which Part 5 of the Act applies, that is, review of certain conduct.

A complaint may be in writing or verbal, but the Privacy Commissioner may require a verbal complaint to be put in writing. The Privacy Commissioner may require information about a complaint to be provided by the complainant in a particular manner, and may require a complaint to be verified by statutory declaration.

A complaint must be made within 6 months (or such later time as the Privacy Commissioner may allow) from the time the complainant first became aware of the conduct or matter that was the subject of the complaint. A complainant may amend or withdraw a complaint.

APPENDIX 1: INFORMATION SHEET FOR INTERNAL REVIEW

Internal review is a process whereby this agency will handle complaints about how it has dealt with personal information.

Under section 53 of the *Privacy and Personal Information Protection (PPIP) Act,* individuals have the right to seek a review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the PPIP Act. This right does not apply to conduct which occurred before July 2000.

The request for review can only be made where it is alleged that the agency has:

- breached any of the information protection principles that apply to the agency
- breached any code made under the Act applying to the agency
- disclosed personal information kept in a public register.

The request for review should be lodged using the Application Form for Internal Review. This application for review should be lodged at an office of the agency within six months from the time the applicant first became aware of the conduct sought to be reviewed.

The Privacy Commissioner will be notified of the application, the progress and findings of the internal review, and will subsequently be notified of the action proposed to be taken by the agency in relation to the matter.

A Reviewing Officer will be appointed to conduct the internal review, which will be completed within 60 days from the day on which the application is received. If the review is not completed within 60 days from the day on which the application was received, the applicant is entitled to make an application to the Administrative Decisions Tribunal for a review of the conduct concerned.

Generally the review will be conducted by way of written submissions. The applicant is entitled to have the services of an interpreter.

The review must recommend any one or more of the following:

- take no further action on the matter
- make a formal apology to the applicant
- take such remedial action as it thinks appropriate
- provide undertakings that the conduct will not occur again
- implement administrative measure to ensure that the conduct will not occur again.

Within 14 days of the completion of the review, the applicant will be notified in writing of:

- the findings of the review (and the reasons for those findings), and
- the action proposed to be taken by the agency (and the reasons for taking that action), and
- the right of the person to have those findings and the agency's proposed action reviewed by the Administrative Decisions Tribunal.

If an applicant is not satisfied with the:

- the findings of the review, or
- the action taken by the agency in relation to the application,

the applicant may apply to the Administrative Decisions Tribunal for a review of the conduct that was the subject of the application for internal review.

Name and address of health service

APPENDIX 2: APPLICATION FOR INTERNAL REVIEW

under Section 53 of the Privacy and Personal Information Protection Act 1998

Application number _____

This form[1] is to be completed by the individual bringing the complaint.

1 Family name _____ First name _____

2 Residential address _____

Suburb/Town _____ Postcode _____

3 Postal address (if different from above) _____

Suburb / Town _____ Postcode _____

4 Describe the complaint

_____
_____
_____
_____

5 When did the conduct you are complaining about occur?

_____

6 When did you become aware of this conduct?

_____

7 What effect did the conduct have on you or another person?

_____
_____
_____

8 What effect could the conduct have on you or another person?

_____
_____
_____

9 What would you like to see the agency do about the conduct?

_____
_____
_____

I understand that details of my application will be referred to the Privacy Commissioner in accordance with section 54(1) of the Privacy and Personal Information Protection Act 1998 and that the Privacy Commissioner will be kept advised of the progress of the review.

Signature of applicant _____ Date ___/___/___

[1] *Privacy NSW* A Guide to Internal Reviews

APPENDIX 3: CHECKLIST FOR INTERNAL REVIEW UNDER S53 OF THE ACT

Application number _____

This form is to be completed by the Privacy Contact Officer.

1 Is the complaint a matter which involves a possible breach of the *Privacy and Personal Information Protection Act* or a code made under the Act?
If yes, go to question 2.
If no, notify the Privacy Commissioner - date of notification ___/___/___
and follow the Complaints Handling process.

2 Date of receipt of request for review ___/___/___

3 Date when 60 day period for completion of the review will elapse ___/___/___

4 Date when the Privacy Commissioner was notified of the request and invited to make submissions ___/___/___

5 Has the applicant provided the necessary information under section 53(3) of the Privacy and Personal Information Protection Act?

Yes / No

6 Identify the relevant IPP, code section or public register provision

_____

7 Name of Reviewing Officer _____
Position _____
Phone _____

8 Preliminary comments in relation to the application (attach submission from Privacy Commissioner)

_____
_____
_____

9 What was the outcome of the review? (attach recommendations from review)

_____
_____
_____
_____

10 Date that the applicant was notified of the outcome of the review, the proposed action and their right to seek a review of the findings within 14 days of the review being completed (attach letter to applicant).

___/___/___

Name of Privacy Contact Officer_____