PRIVACY MANAGEMENT PLAN

September 2015
1. Introduction

1.2 Purpose
The Macquarie University Privacy Management Plan (the Plan) informs students, staff, and members of the public about the personal and health information the University collects, holds, manages, uses, and discloses, and how the University is implementing the privacy principles set out in the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA) and the Health Records and Information Privacy Act 2002 (NSW) (HRIPA) (in this document, collectively referred to as the Privacy Acts).

1.3 Scope
The University has developed this Plan in accordance with section 33 of PPIPA. This Plan documents the requirements placed on the University by the Privacy Acts, and outlines how the University intends to protect personal and health information in accordance with these. The Plan applies to the University’s records which contain personal and health information of staff, students, and members of the public. This includes all forms of information, for example, email, soft and hard copies of documents, databases, online and paper-based forms, and in certain circumstances includes verbal communication also.

The University’s offices and units must collect, hold, manage, use, and disclose this information in accordance with this Plan. The Plan provides guidance to University staff on the procedures in place to enable staff to meet the obligations set by PPIPA and HRIPA. All University staff have an obligation to implement the privacy principles established by PPIPA and HRIPA in their day-to-day practices, by complying with the Acts in the course of collecting, managing, using, and disclosing personal and health information. University staff should refer to the Plan as a key privacy resource, and contact Privacy Officer for advice relating to privacy matters, via privacyofficer@mq.edu.au or (02) 9850 4587.

The University is not required to comply with the Australian Privacy Principles in the Privacy Act 1988 (Cth) as it is not an ‘organisation’ within the meaning of the Act. The University is, however, a ‘file number recipient’ for the purposes of the Privacy Act because it holds records of employees which contain tax file number information. As such, the University must comply with any rules relating to tax file number information issued under section 17 of the Privacy Act.

The University’s controlled entities, as private sector organisations, are subject to the Privacy Act 1988 (Cth) and the HRIPA. The University must ensure that any information provided by the University to another organisation is protected to the same standards that the University applies to the information it holds. Therefore, in any dealings between the University and its controlled entities in relation to personal and health information, the standards applicable to the University (i.e. under PPIPA and HRIPA) must be applied. The University must also meet these standards in its dealings with affiliates and contractors.

1.3 Section 41 Directions
Under s41 of PPIPA, the Privacy Commissioner may make a direction or modify the requirement for an agency to comply with an IPP or a code of practice. The directions that apply to the University are:

- **Direction relating to the Information Transfers between NSW Public Sector Agencies** (provides certain exemptions to the PPIPA where exchanges of information between agencies are reasonably necessary for responses to correspondence from Ministers or MPs; referral of inquiries; auditing accounts or performance of programs administered by agencies; law enforcement purposes not covered by exceptions in the PPIPA; performance agreements between agencies)

- **Direction relating to the Processing of Personal Information by NSW Public Sector Agencies in relation to their Investigative Functions** (provides certain exemptions to the PPIPA for the proper exercise of any investigative functions or conduct of any lawful investigations)

- **Direction relating to the Disclosures of Information by NSW Public Sector Agencies for Research Purposes** (provides certain exemptions to the PPIPA for: research where a research ethics committee exists and considers privacy issues in its approvals for research; in relation to personal information contained in records deposited for purposes that include research; in relation to the collection and use of personal information to provide reference material to collections of historical or cultural significance)

The full text of these Directions can be found at the [IPC website](http://ipc.nsw.gov.au).

### 1.4 Complaints

The Plan contains information on how to make a complaint about a privacy issue and how to seek a formal Internal Review by the University where a breach of privacy is suspected. A pro forma is attached to this Plan [page 39].

Any comments or queries about the Plan should be forwarded to the Privacy Officer, via email at [privacyofficer@mq.edu.au](mailto:privacyofficer@mq.edu.au), or phone on (02) 9850 4587.

### 2. Definitions

#### 2.1 Personal Information

The PPIPA defines personal information, in s 4(1), as:

‘information or an opinion (including information or an opinions 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. Personal information includes such things as an individual’s fingerprints, retina prints, body samples or genetic characteristics...’

The University holds personal information in a range of forms, for example, paper-based formats, visual formats including photographs and other image formats, video and film footage, voice recordings, computer-based storage including databases, fingerprint...
images, human tissue and DNA samples.

2.2 Health Information

The HRIPA defines health information, in s 6, as ‘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 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, or

(e) healthcare identifiers’

2.3 Exceptions

Both the PPIPA and HRIPA exclude the following categories of information from their scope:

i) Information about an individual who has been dead for more than 30 years

ii) Information about an individual that is contained in a publicly available publication

   Personal information, once it is contained in a publicly available publication, ceases to be covered by the PPIPA

   o This can include, for example, information which is published in newspapers, books, or on the Internet (including social media platforms), broadcast on radio or television, or made known at a public event such as a graduation ceremony

iii) Information or an opinion about an individual’s suitability for appointment or employment as a public sector official

   o Information relating to the suitability for employment as a University staff member is excluded from the Privacy Acts. This includes pre-employment checks such as information contained in a resume, selection report, references for appointment or promotion; it also includes disciplinary records.

   o Other employee information constitutes personal information to which the PPIPA and HRIPA apply. This includes, for example, staff training records, leave and attendance records.
3. Types of personal and health information held by the University

In undertaking its learning and teaching, research, and community engagement functions, the University collects, stores, and uses a broad range of personal and health information relating to its students, staff, and members of the public.

Requests by individuals to access their information under the PPIPA should be directed to the Privacy officer [page 38].

The primary types of information held by the University are outlined below (this is not an exhaustive list):

**Students**
The University collects and holds information to support its functions related to learning and teaching and student administration (admission, enrolment, assessment, personal welfare, misconduct, and graduation).

This includes (but is not limited to):
- Personal identifiers (e.g. names, student identification numbers, contact details)
- Digital photos of students, collected for the purpose of creating student identification cards
- Financial information (e.g. tax file numbers, HECS information, information relating to student loans)
- Student welfare information (e.g. health and medical information, including supporting evidence for Disruption to Studies applications, disability and equity information)
- Assessment information (including examiners’ reports, practicum assessments, etc)

The University holds learning and teaching and student administration related personal information in a range of locations, forms, and formats:
- enrolment, admission, and progression information is primarily stored in Student1 and Tracker (the University’s student administration and CRM systems, respectively). This includes information relating to units of study (both attempted and completed); prizes and scholarships awarded; program completion and graduation.
- Faculties, Departments, and individual staff members will also hold information relevant to the delivery of their learning and teaching duties (e.g. class lists, assessment records)
- the University’s learning management system (Moodle/iLearn) contains student names and identifiers, records of online class discussions, communications between students and academic staff, assessments, and assessment records
- the University Library holds records on students in order to identify users and facilitate Library privileges for students
- University Security retain records relating to car parking permits, CCTV
Staff
The University collects and retains information on all staff relating to their employment (primarily, information relating to the hiring and management of staff, and workers’ compensation). This includes (but is not limited to):

- personal identifiers (e.g. names, staff identification numbers, contact details)
- digital photos of staff, collected for the purpose of creating staff identification cards
- financial information (e.g. tax file declarations, banking details, remuneration details)
- staff welfare information (e.g. health and medical information related to employment including sick leave documentation; Workers Compensation and Occupational Health and Safety files; disability and equity information)
- staff communications

The University’s staff records are collected and stored primarily as follows:

- most staff information is held in the University’s Human Resources electronic information management systems; and in staff files
- information contained in University ICT systems (including staff email and other University accounts)
- the University Library holds records on staff in order to identify users and facilitate Library privileges for staff
- University Security retains records relating to car parking permits, CCTV footage, and incident notifications and reports
- some staff information is publically accessible. For example, the University’s publically accessible staff directory provides current staff members’ name, position, University telephone number, office location and University email address. Some of the University’s publications (e.g. the annual report) also contain some staff information (such as names, position held, and qualifications)

Others
The University holds a range of personal information about individuals who are not staff or students of the University. This includes potential students; alumni; benefactors; external members of the University’s governance bodies; consultants, contractors, and others engaged in business with the University; users of the University’s medical and health services; and users of the University’s Library services.

Video surveillance is used across campus, to facilitate the security and safety of all people on campus. The University’s CCTV cameras are visible and operate inside and outside buildings on campus. Signage is placed across campus to advise students, staff, and visitors that CCTV is in use.

Some of the University’s research and teaching activities involve the collection of data of people outside the University, and which contains personal information (this may be held by the University or by individual researchers). Human-based research projects require approval by the University’s Human Ethics Research Committee (HREC), and as part of this process, consent is obtained in order to collect and use
identifiable personal information for research.

Some records of the University’s governance bodies (particularly Council, and Senate and its subcommittees) may refer to personal information relating to external persons (as well as in relation to University staff and students).

The University’s business dealings will involve the collection, storage and use of personal information. For example, procurement records will contain information about suppliers and vendors.

**Health information**

In addition to the above instances where the University may collect and manage health information in relation to its learning, teaching, research, and administrative functions, the University collects and manages health information as a provider of certain health services. The University’s medical service providers (including the hospital, clinics, and Campus WellBeing medical and counselling services) collect and retain health information in records relating to their patients (including staff, students, and others). The University also collects health related information in relation to its education and training of health care professionals (e.g. information related to clinical practice undertaken by students). Health information is managed in accordance with the HRIPA (refer to section 5 of the Plan).

4. The Privacy Principles

The PPIPA and HRIPA contain principles that govern the protection of personal information. The PPIPA sets out information protection principles that cover the collection, storage, access, accuracy, use, and disclosure of personal and health information. The health privacy principles contained in the HRIPA cover the use of identifiers to protect identity, the consent to link health records of an individual, the right to anonymity in receiving health services, and the flow of information across the NSW border.

The University must comply with these principles in order to meet its legal obligations under the Privacy Acts.

The full text of the personal information principles is set out in appendix 1, and the full text of the health information principles is set out in appendix 2.

Sections 4.1 and 4.2 below set out the obligations that the University will meet in managing personal and health information. Further guidance on how to apply these principles is set out in the suite of guidelines, procedures, and interactive flowcharts that support this Plan.

**4.1 Information Protection Principles (IPPs)**

The IPPs cover the collection, storage, access and amendment, use, and disclosure of personal information as follows:
Collection
The University must only collect personal information for a lawful purpose that is directly related to a function or activity of the University, and the collection of the information is reasonably necessary for that purpose. These purposes include, primarily, functions relating to admission, enrolment, progression, and gradation of students (including teaching); communication with prospective students and alumni; selection, appointment, management, and payment of staff; research; and business dealings that support the functions of the University.

Personal information may only be collected by lawful means (i.e. in accordance with the Privacy Acts and other legislation applicable to the context in which the information is being collected). Wherever possible, the University must collect personal information directly from the individual the information relates to. Individuals can authorise the collection of information from others. For example:

- UAC applicants authorise the University to collect their application information for the purposes of assessment for an offer of a place in a course offered by the University
- Parents of children under 16 can provide this information on behalf of their children.

When deciding to collect personal information, the University must consider the relevance, necessity, and accuracy of the information, and take care to be non-intrusive on the personal affairs of individuals from whom information is being sought. For example, students submitting Disruption to Studies notifications are asked to provide documentation stating the impact of the disruption on their ability to complete an assessment; the nature of the disruption (or condition causing the disruption) is not required.

The University must take reasonable steps to ensure that the person whose information is being collected is aware of the fact of collection. The University must inform individuals of:

- the reason for the collection of the information
- who is collecting the information (and provide contact details)
- which other parties the information being collected is usually disclosed to
- how the individual can access and correct the information being collected

The University informs individuals of the above through its collection notices (available on the University’s Privacy webpages), and through privacy statements and consent forms as required.

Where the supply of information is voluntary (i.e. it is not required by law), the University must allow the individual to refuse to supply the information, and explain the consequences of not supplying it. For example, in the terms and conditions of enrolment, the University explains that admission and enrolment cannot proceed without particular information being provided by prospective students.

In cases where information being sought is required by law, the legal basis of this request must clearly communicated to the individual.
Storage

The security of personal information collected by the University must be ensured, whether this information is in computer or online systems, or in paper-based form. This means that personal information must be protected from unauthorised access, alteration, and use.

The University must implement reasonable safeguards to protect against loss, unauthorised access, use, modification, disclosure, and any other misuse of the personal information it holds. The University has controls in place to manage the information it stores (for example, period review of access to online systems in which personal information is stored). Additionally, the University must only retain information for as long as it is necessary for the purposes for which it can lawfully be used, and ensure the secure disposal of information once it is no longer needed.

ICT systems

The University stores information on computers and with IT service providers who have contracted with the University. IT service providers often route information through other jurisdictions as a way of storing information. Whilst it is not possible for the University to nominate the particular country where this information is stored or transmitted, the University ensures contractually that the information is protected securely and that the contract provider has a privacy policy which protects the information from being accessed without authorisation.

If it is necessary for the University to provide personal information to a person in connection with the provision of a service to the University, the University must do everything reasonably within its power of to prevent unauthorised use or disclosure of the information.

Accuracy, access and amendment

The University must take reasonable steps to ensure the information it holds and uses is relevant, accurate, up to date, and not misleading, having regard for the purposes for which it was collected and any purpose(s) directly related to that purpose (this is considered the primary purpose of collection).

Individuals have a right to know:

- whether information about them is held by the University
- the nature of this information
- the purpose(s) for which it is being used
- how they can access their information (and ensure valid requests for access proceed without excessive delay or expense)
- how they can correct this information if it is not accurate

Students can view and update their personal information collected as part of the admission and enrolment process via eStudent, or by contacting Student Connect. Staff can contact HR to correct or update some of their personal information in HROnline.
All other requests should be directed to the Privacy Officer.

Note that access to information about a third party is not accessible under the Privacy Acts.

Use

The use of personal information held by the University is limited to the purpose(s) for which it was collected, unless an individual has consented to the information being used for another purpose. Information may only be used for another purpose without an individual’s consent if:

- it is being used for another purpose directly related to the purpose for which the information was collected
- it is necessary to prevent or lessen a serious and imminent threat to the life or health a person
- it is reasonably necessary for law enforcement purposes or for the protection of public revenue.

The University must also take reasonable steps to ensure that the information it holds is relevant, accurate, up to date, and not misleading, having regard for the purpose(s) for which the information is to be used.

The general uses of personal information collected by the University are described in the University’s privacy collection notices (available at the Privacy webpages). Privacy statements and/or consent forms are provided where the collection of information is outside the parameters of these privacy collection notices.

The University takes reasonable steps to ensure that personal information is accessible only by those staff members who need to access it in order to carry out their duties. Information collected by the University may be used by offices and units that did not undertake the initial collection of the information, if this is for the same purpose or directly related to a purpose for which it was originally collected.

Disclosure

The University does not disclose personal information it holds about students, alumni, staff, or members of the public to external third parties without the individual’s express consent unless it is legally authorised or required to do this.

The disclosure of personal information held by the University is limited to the primary purpose(s) for which it was collected, subject to the following exceptions:

- where the disclosure is for a purpose directly related to the purpose for which the information was collected, and the University has no reason to believe that the individual would object to the disclosure
- where an individual has been made aware, or is likely to be aware, that information of that kind is usually disclosed to the body or person that the
University wishes to disclose the information to

- where the University believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of a person
- where the disclosure is permitted by a Public Interest Direction made by the NSW Privacy Commissioner (see section 1.3 of this Plan)

For example, where the University offers academic programs in conjunction with another institution, we may need to exchange personal information with these institutions in order to facilitate student enrolment and progression through the program. In some instances, the University may be required to release information to third parties by law. The University is required by law to release information to government agencies such as the Department of Education, Employment and Workplace Relations (DEEWR) and the Department of Immigration and Border Protection (DIBP) if requested under a relevant section of legislation that governs the Departments.

The University also has discretion to, and can be required to, release information in relation to law enforcement:

- in relation to proceedings for an offence including in response to a subpoena or search warrant
- to a law enforcement agency in relation to a person reported as missing
- if reasonably necessary for the protection of public revenue or to investigate an offence where there are reasonable grounds to believe that an offence has been committed

**Sensitive Information**

There are stricter obligations for the disclosure of personal information relating to an individual’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health, and sexual activities. This information cannot be disclosed unless it is reasonably necessary for law enforcement purposes, or if the disclosure is necessary to prevent a serious or imminent threat to the life or health of a person.

In addition, this information cannot be disclosed to a person or body in a jurisdiction outside NSW unless a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction, or the disclosure is permitted under a privacy code of practice.¹

¹ Currently, the University does not have a code of practice and as such, the IPPs apply in full to the University. There are exceptions such as for providing services or assistance to specific groups of students, or if another act requires the disclosure (see s.25 of the PPIP Act).
4.2 Health Privacy Principles (HPPs)

Health information, along with personal information collected by the University in the context of providing a health service, is governed by the HPPs set out in the HRIPA.

The HRIPA sets out strict rules for disclosure and use of health information by and within the University. The University must only collect health information for a lawful purpose that is directly related its functions and activities, where the information is reasonably necessary these purposes. Unless it is impractical or unreasonable to do so, the information must be collected from the individual to who the information relates. The University must also take reasonable steps to ensure that health information collected is not misleading or excessive, that the collection does not intrude unreasonably on the personal affairs of the individual, is accurate and complete, and up to date.

Health information held by the University must be held securely, and protected against loss, unauthorised access, use, modification, disclosure, or other misuse. The use of identifiers (e.g. a number assigned to an individual’s health information for the purpose of uniquely identifying them) should only be used if it is reasonably necessary for the University’s functions related to the handling of health information. Unless legally required or authorised to, the University must not include health information about any individual in a health records linkage system without their consent (this includes for research purposes noted above).

The University must take reasonable steps to ensure that an individual\(^2\) is aware of the purpose(s) for which their health information is being collected (including any legal requirements to collect this information), whether it is likely to be disclosed to others, and how to request access to the information held about them. The University must also enable an individual to ascertain whether it holds any health information about them.

An individual can refuse to provide health information being requested by the University unless there is a legal requirement to provide this information. The University must inform the individual about any consequences of not providing the requested information (for example, the impact on the ability of the University to provide the individual with the services for which the information is being sought). Individuals also have the right to receive health services without identifying themselves where this is practicable and lawful.

Generally, an individual’s health information cannot be disclosed by the University for any purpose other than the primary purpose for which it was collected. There are a limited

\(^2\) Or, if the individual is incapacitated, the individual’s authorised representative.
number of exceptions to this rule. Health information relating to an individual can be used or disclosed in relation to a secondary purpose in the following situations:

- the University has obtained consent from the individual
- it is used for a related health treatment or research purpose within the reasonable expectations of the individual
- in relation to suspected unlawful activity, unsatisfactory professional conduct, or breach of discipline
- in relation to a serious threat to the health, safety, or welfare of the individual or public health or safety
- there are compassionate grounds for disclosure
- where necessary to find a missing person
- for law enforcement purposes, or if the information is lawfully authorised or required to be disclosed by another law
- it is reasonably necessary for the management of health services, training and educating health service providers, or research activities subject to the following conditions:
  - it is impractical to seek consent for this use from the individual to whom the information relates
  - the use of de-identified data is not practicable (but ensuring that the data is de-identified as far as possible)
  - the information is not published in a generally available form that might enable individuals to be identified
  - and any guidelines issued by the Information Privacy Commission are complied with
- where the NSW Work Health and Safety legislation requires disclosure of information that is necessary for the reduction of health and safety risk in the workplace

The HRIPA also sets out obligations in relation to the transfer of information across NSW borders. Without the individual’s consent, the University can only transfer health information outside NSW (including to a Commonwealth agency) in the following circumstances:

- the recipient of the information is subject to health privacy provisions similar to NSW (i.e. that accord with the HRIPA)
- the transfer is part of an agreed contract in the interests of the individual
- the transfer benefits the individual, and it is impractical to obtain consent, and the individual would likely agree with the transfer
- the transfer will lessen or prevent a serious and imminent threat to the health, safety, or welfare of a person, or to public health or safety
- steps have been taken to ensure that the information will not be used or disclosed contrary to the HPPs
- the transfer is required or permitted by law
5. Complaints and Reviews

The University is committed to protecting the privacy of personal and health information in accordance with privacy legislation. If you have concerns about the way in which the University has managed your personal or health information, we encourage you to contact the Privacy Officer as soon as possible to discuss the issue (privacyofficer@mq.edu.au, or (02) 9850 4587).

Internal Reviews

The University may undertake an internal review to deal with formal complaints where it is alleged that there is a breach of the Privacy Acts. Formal complaints and applications for review must be made in writing, and directed to the Privacy Officer within 6 months of the time the individual became aware of the alleged breach. Formal complaints must be made using the form provided at appendix 4.

Upon receipt of a formal application for review, the Chief Operating Officer (or delegate) will appoint a staff member of the University to undertake the review. This will be a person who has not had substantive involvement in the matter which gave rise to the complaint. In processing the review, the University follows the guidelines provided by the NSW Information and Privacy Commissioner, available online at


Internal reviews will be completed within 60 days of the receipt of a formal application for review, and the applicant informed of the outcome of the review within 14 days of its completion. The outcomes of an interview review include:

- taking no further action, if the University is satisfied that no breach has occurred
- implementing controls to prevent recurrence of a breach, or undertaking actions to prevent the conduct from recurring
- making a formal apology to the applicant
- taking appropriate remedial action
- providing an undertaking that the conduct will not recur

The University will also inform the NSW Privacy Commissioner of formal complaints it receives, and provide reports to the Commissioner on the progress of its investigation into these matters.

External Reviews
If a person believes their privacy has been breached, a complaint can also be made to the NSW Privacy Commissioner. This can be done without engaging the University’s internal review process.

An applicant can also take the matter to the NSW Administrative Decisions Tribunal (NSW ADT) if the University has not completed an internal review within 60 days of the application date. If an applicant is not satisfied with the outcome of the University’s internal review, they can apply to the NSW ADT to review the decision. Finally, if the applicant is not satisfied with the determination of the NSW ADT, they have a right of appeal to the Appeal Panel of the NSW ADT.

6. Staff Privacy Training and Support

The University’s Privacy Management Plan is supplemented by a suite of tools to assist staff in identifying when a process, activity, or project might involve personal or health information, and how to operationalise our obligations around the collection, use, disclosure and overall management of this information in various contexts.

The University will also provide regular training and education seminars to staff to inform them of their responsibilities under the Privacy Acts.

The Privacy Officer monitors the landscape in relation to privacy. Privacy news and updates are communicated to all staff via the This Week at Macquarie electronic staff newsletter.

The Privacy Officer (with advice from a University solicitor as appropriate) will also provide tailored advice to University staff to support them in understanding and meeting their privacy obligations. For example, the Privacy Officer can provide advice about:

- whether personal information is being collected for a lawful purpose
- if that lawful purpose is directly related to a function of the University
- whether or not the collection of that personal information is reasonably necessary for the specified purpose.

As part of meeting our obligations, this Plan will be reviewed at 12-month intervals to ensure it reflects both the privacy obligations the University must meet, and our practices around the management of personal and health information.
Appendices
How to seek a formal Internal Review by the University where a breach of privacy is suspected. A pro forma is attached to this Plan

All other requests for personal information should be directed to the Privacy Officer using the form provided in appendix 4.

Appendices
Appendix 1: Information Protection Principles
Appendix 2: Health Privacy Principles
Appendix 3: Application For Access to Personal Information
Appendix 4: Application for review of conduct under section 53 of the Privacy and Personal Information Protection Act 1998
Appendix 5: Draft letter to the Privacy Commissioner regarding receipt of application for internal review under section 53
Appendix 6: Internal Review Checklist
Appendix 1 – Information Protection Principles

Privacy and Personal Information Protection Act 1998 (NSW) Part 2 Division 1

8 Collection of personal information for lawful purposes

(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.

9 Collection of personal information directly from individual

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.

10 Requirements when collecting personal information

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,
11 Other requirements relating to collection of personal information

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.

12 Retention and security of personal information

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

(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.

13 Information about personal information held by agencies

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.

14 Access to personal information held by agencies

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.

15 Alteration of personal information

(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.

(4) This section, and any provision of a privacy code of practice that relates to the requirements set out in this section, apply to public sector agencies despite section 25 of this Act and section 21 of the State Records Act 1998.

(5) The Privacy Commissioner's guidelines under section 36 may make provision for or with respect to requests under this section, including the way in which such a request should be made and the time within which such a request should be dealt with.
In this section (and in any other provision of this Act in connection with the operation of this section), "public sector agency" includes a Minister and a Minister's personal staff.

16 Agency must check accuracy of personal information before use

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.

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.
(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.

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 or sexual activities unless the disclosure is necessary to prevent a serious and 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 or to a Commonwealth agency unless:

   (a) a relevant privacy law that applies to the personal information concerned is in force in that jurisdiction or applies to that Commonwealth agency, 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 to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales and to Commonwealth agencies.

(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 later.
Appendix 2 – Health Privacy Principles

*Health Records and Information Privacy Act 2002 (NSW) Schedule 1*

1 Purposes of collection of health information

(1) An organisation must not collect health information unless:

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and

(b) the collection of the information is reasonably necessary for that purpose.

(2) An organisation must not collect health information by any unlawful means.

2 Information must be relevant, not excessive, accurate and not intrusive

An organisation that collects health information from an individual 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.

3 Collection to be from individual concerned

(1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

(2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

4 Individual to be made aware of certain matters

(1) An organisation that collects health information about an individual from the individual must, at or before the time that it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the following:

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

(b) the fact that the individual is able to request access to the information,
(c) the purposes for which the information is collected,

(d) the persons to whom (or the types of persons to whom) the organisation usually discloses information of that kind,

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

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

(2) If an organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is generally aware of the matters listed in subclause (1) except to the extent that:

(a) making the individual aware of the matters would pose a serious threat to the life or health of any individual, or

(b) the collection is made in accordance with guidelines issued under subclause (3).

(3) The Privacy Commissioner may issue guidelines setting out circumstances in which an organisation is not required to comply with subclause (2).

(4) An organisation is not required to comply with a requirement of this clause if:

(a) the individual to whom the information relates has expressly consented to the organisation not complying with it, or

(b) the organisation is lawfully authorised or required not to comply with it, or

(c) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998), or

(d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or

(e) the information concerned is collected for law enforcement purposes, or

(f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

(5) If the organisation reasonably believes that the individual is incapable of understanding the general nature of the matters listed in subclause (1), the organisation must take steps that are reasonable in the circumstances to ensure that any authorised representative of the individual is aware of those matters.

(6) Subclause (4) (e) does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.
(7) The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

5 Retention and security

(1) An organisation that holds health information must ensure that:

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

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

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

Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

(2) An organisation is not required to comply with a requirement of this clause if:

(a) the organisation is lawfully authorised or required not to comply with it, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

(3) An investigative agency is not required to comply with subclause (1) (a).

6 Information about health information held by organisations

(1) An organisation that holds health information must take such steps as are, in the circumstances, reasonable to enable any individual to ascertain:

(a) whether the organisation holds health information, and

(b) whether the organisation holds health information relating to that individual, and

(c) if the organisation holds health information relating to that individual:

(i) the nature of that information, and

(ii) the main purposes for which the information is used, and
(iii) that person’s entitlement to request access to the information.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

### 7 Access to health information

(1) An organisation that holds health 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. Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. Access to health information held by public sector agencies may also be available under the *Government Information (Public Access) Act 2009* or the *State Records Act 1998*.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

### 8 Amendment of health information

(1) An organisation that holds health 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 health 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 an organisation is not prepared to amend health information under subclause (1) in accordance with a request by the individual to whom the information relates, the organisation 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 health information is amended in accordance with this clause, 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 organisation. Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. Amendment of health information held by public sector agencies may also be able to be sought under the Privacy and Personal Information Protection Act 1998.

(4) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

9 Accuracy

An organisation that holds health 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.

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 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
(c1) the information is genetic information and the use of the information for the secondary purpose:

(i) is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative of the individual to whom the genetic information relates, and

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

(g) the use of the information for the secondary purpose is by a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(h) the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the Health Practitioner Regulation National Law (NSW), or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or
(i) the use of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(j) the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(k) the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

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 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.

(c) the disclosure 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

(c1) the information is genetic information and the disclosure of the information for the secondary purpose:

   (i) is to a genetic relative of the individual to whom the genetic information relates, and

   (ii) is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative of the individual to whom the genetic information relates, and

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

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

(e) the disclosure 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 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) if the information could reasonably be expected to identify the individual, the information is not made publicly available, 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

(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, or

(h) the disclosure of the information for the secondary purpose is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(i) the organisation:

   (i) has reasonable grounds to suspect that:

      (A) unlawful activity has been or may be engaged in, or

      (B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the Health Practitioner Regulation National Law (NSW), or

      (C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

   (ii) discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(j) the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(k) the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(l) the disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.
(2) An organisation is not required to comply with a provision of this clause if:

   (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or

   (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998), or

   (c) the organisation is an investigative agency disclosing information to another investigative agency.

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

   (a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or

   (b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) If health information is disclosed in accordance with subclause (1), the person, body or organisation to whom it was disclosed must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

(6) The exemptions provided by subclauses (1) (k) and (2) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

12 Identifiers

(1) An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

(2) Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

   (a) the individual has consented to the adoption of the same identifier, or
(b) the use or disclosure of the identifier is required or authorised by or under law.

(3) Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)-(k) or 11 (1) (c)-(l), or

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

(c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

(4) If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either:

(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency, or

(b) use or disclose an identifier of the individual that has been assigned by the public sector agency.

13 Anonymity

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

14 Transborder data flows and data flow to Commonwealth agencies

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or

(b) the individual consents to the transfer, or
(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or

(e) all of the following apply:

   (i) the transfer is for the benefit of the individual,

   (ii) it is impracticable to obtain the consent of the individual to that transfer,

   (iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the transfer 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

(g) the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles, or

(h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

15 Linkage of health records

(1) An organisation must not:

   (a) include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included, or

   (b) disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

(2) An organisation is not required to comply with a provision of this clause if:

   (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*), or

(c) the inclusion of the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual is to be disclosed) is a use of the information that complies with HPP 10 (1) (f) or a disclosure of the information that complies with HPP 11 (1) (f).

(3) In this clause: "**health record**" means an ongoing record of health care for an individual. "**health records linkage system**" means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.
Appendix 3 - Application for access to personal information

You can request to access personal information about you under s14 of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIPA). Requests must be made in writing, using this form. If you need help in filling out this form, please visit the University’s privacy pages for more information and contact details (http://www.mq.edu.au/privacy).

Once completed, post this form to:
Privacy Officer, Macquarie University NSW 2109, Australia

Applicant’s details

<table>
<thead>
<tr>
<th>Title</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td></td>
</tr>
<tr>
<td>Postal Address</td>
<td></td>
</tr>
<tr>
<td>Telephone number</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td></td>
</tr>
</tbody>
</table>

Please detail your request for personal information about you held by the University:


Applicant’s signature: ................................................. Date:..............................

Privacy statement: you are not required to provide the information sought on this form, but if you do not provide all the information requested, the University may not be able to process your request. The information on this form will be used by the University’s staff in order to process your request and will not be disclosed outside the University without your express consent (except where required or authorised by law). Any enquiries regarding access to, or correction of, personal information about you held by the University should be addressed to the Privacy Officer.
Appendix 4 – Application for review of conduct under section 53 of the *Privacy and Personal Information Protection Act 1998*

**Notification of privacy compliant**
You can make a complaint relating to the management of your personal information under s53 of the *Privacy and Personal Information Protection Act 1998* (NSW). (PPIPA) If you need help in filling out this form, please visit the University’s privacy pages for more information and contact details ([http://www.mq.edu.au/privacy](http://www.mq.edu.au/privacy)).

**Applicant’s details**

<table>
<thead>
<tr>
<th>Title</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Surname</td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td></td>
</tr>
<tr>
<td>Postal Address</td>
<td></td>
</tr>
<tr>
<td>Telephone number</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td></td>
</tr>
</tbody>
</table>

**Details of the complaint** (Use continuation sheets if necessary)

What is the conduct complained of?

---

39
When did the conduct you are complaining about occur? (Use dates if possible)

When did you become aware of this conduct?

What effect did the conduct have on you or another person?
What would you like to see the University do about the conduct?

Declaration and signature
I understand the details of my complaint will be referred to the Privacy Commissioner in accordance with section 54 of the PPIPA, and that the University will advise the Privacy Commissioner of the progress and outcome of the University’s review of my complaint.

Signature: ................................................... Date: ............................

Applicant’s signature: ................................................................. Date: ............................

Once completed, post this form to:
Privacy Officer, Macquarie University NSW 2109, Australia

Office use only
Date received: .................................................................

File reference: .................................................................

Privacy statement: you are not required to provide the information sought on this form, but if you do not provide all the information requested, the University may not be able to process your request. The information on this form will be used by the University’s staff in order to process your request and will not be disclosed outside the University without your express consent (except where required or authorised by law). Any enquiries regarding access to, or correction of, personal information about you held by the University should be addressed to the Privacy Officer.
Appendix 5 – Draft letter to the Privacy Commissioner regarding receipt of application for internal review under section 53

File number:

Date

Dr Elizabeth Coombs
NSW Privacy Commissioner
GPO Box 7011
Sydney NSW 2001

Dear Dr Coombs,

Notification in accordance with s. 54(1) of the NSW Privacy and Personal Information Protection Act of 1998.

The University has received an application for Internal Review under s. 53 of the Privacy and Personal Information Protection Act 1998. A copy of the letter of application is attached.

The matter is being investigated. I shall keep you informed of the progress and outcome of the review.

Should you have any submissions regarding this matter, please send them to me at the above address.

Yours sincerely,

Privacy Officer
Appendix 6 – Internal Review Checklist
Updated July 2014

The Privacy and Personal Information Protection Act 1998 (PPiP Act) and the Health Records and Information Privacy Act 2002 (HRiP Act) provide that public sector agencies deal with complaints by way of Internal Review. This process is the same under both Acts although you will be assessing the alleged conduct against different standards (the IPPs and the HPPs).

A privacy complaint may come under:

- the PPIP Act, section 53, if it relates to personal information, and the Information Protection Principles (IPP); or
- the HRiP Act, section 21, if it relates to health information and the Health Privacy Principles (HPP).

Notes: The 12 information protection principles (IPP) in the PPIP Act are legal obligations the manner in which NSW government agencies (including statutory bodies and local councils) must handle personal information. The 12 IPP cover the collection, storage, use and disclosure of personal information as well as access and correction rights.

The 15 health privacy principles (HPP) in the HRiP Act are legal obligations describing the manner in which NSW public sector agencies and private sector organisations and individuals, such as businesses, private hospitals, GPs, gyms and so on must handle health information. The 15 HPP prescribe what an organisation must do when it collects, stores, uses and discloses health information. The HPP also cover access and correction rights.

s.53(1): a person (the applicant) who is aggrieved by the conduct of a public sector agency is entitled to a review of that conduct. The requirements for an application for internal Review are as follows:

s. 53(3): An application for such a review must: (a) be in writing, and (b) be addressed to the public sector agency concerned, and (c) specify an address in Australia to which a notice under subsection (8) may be sent, and (d) be lodged at an office of the public sector agency within six months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct the subject of the application, and (e) comply with such other requirements as may be prescribed by the regulations (there are no additional requirements prescribed at this time.)

Preliminary steps

1. Is the complaint about a person’s personal information?

☐ Yes – you should treat their complaint as a request for Internal Review. Go to Q.2.

☐ No – follow your agency’s normal complaint handling procedures.
Note: “Personal information” is defined at s.4 of the PPIP Act as “information or an opinion... about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion”. There are some exemptions to the definition (e.g. for “information or an opinion about an individual’s suitability for appointment or employment as a public sector official”) so check s.4 in full. However if you are thinking of relying on one of these exemptions, especially s.4(3)(b) or s.4(3)(j), please first seek advice from the Information and Privacy Commission NSW (IPC) as to the extent to which the exemption applies.

2. Is the complaint about a person’s health information?

[ ] Yes – you should treat their complaint as a request for Internal Review under the HRIP Act. This means that the HPPs and other standards under the HRIP Act will apply.

[ ] No – you should treat their complaint as a request for Internal Review under the PPIP Act. This means that the IPPs and other standards under the PPIP Act will apply.

[ ] Both – See the notes below.

Notes: “Health information” is defined at s.6 of the HRIP Act as “personal information that is information or an opinion about the physical or mental health or a disability of an individual; express wishes about the future provision of health services; a health service provided or to be provided; any other personal information collected to provide or in providing a health service”. The definition also includes information having to do with organ donation and genetic information. There are some exemptions to the definition in s.5 of the HRIP Act (e.g. for “information or an opinion about an individual’s suitability for appointment or employment as a public sector official”) so check the Act. However if you are thinking of relying on one of these exemptions, especially s.5 (3)(b) or s.5 (3)(m), please first seek advice from the IPC as to the extent to which the exemption applies.

If it is easy to distinguish between what is health information and what is other personal information then apply the relevant Act to each piece of information the subject of the complaint. If it is unclear which Act should apply, or it is too difficult to deal with the information in distinct parts, then in our view, it is best to take a cautious approach and apply both Acts to all the information the subject of the complaint.

3. According to the complainant, when did the alleged conduct occur?

____________________ - ________________

4. Is the complaint about conduct that occurred after 1 July 2000?

[ ] Yes – go to Q.5.

[ ] No – the PPIP Act does not apply. Follow your agency’s normal complaint handling procedures.
5. Is the complaint about health information and conduct that occurred after 1 September 2004?

☐ Yes – the HRIP
     Act covers this complaint.

☐ No – the PPIP
     Act covers this complaint.

6. According to the complainant, when did they first become aware of the alleged conduct?

__________________ - __________________

Note: that in Y v DET, the ADT warned against agencies using ‘self-serving calculations’ when determining the date on which the complainant may have first become aware of the conduct complained of.

7. When was this application / privacy complaint first lodged?

__________________ - __________________

Note: In Y v DET, the ADT found that “express reference” to the PPIP Act is not essential in correspondence with agencies, especially where the context suggests that a statutory right is being invoked. Therefore the complainant need not have used the phrase ‘Internal Review’ for their privacy complaint to be considered by law to be an Internal Review application. Agencies should therefore look to the date the first written complaint about a breach of privacy was made.

8. If more than six months lapsed between the date at Q.6 and the date at Q.7, your agency must decide whether you will accept a late application.

Will you accept this late application?

☐ Yes – go to Q.9.

☐ No – explain your reasons as to why you are unable to accept this older than six months complaint to the complainant, then follow your agency’s normal complaint handling procedures.

Note: Your agency should have a clear and written policy on the grounds under which you will allow a late application, including the means by which you will notify complainants about those grounds and what the complainant must prove to you. Include your policy in your Privacy Management Plan.

9. When will 60 days elapse from the date at Q.7?

__________________ - __________________
After this date the complainant has 28 days to go to NSW Civil and Administrative Tribunal (the Tribunal) without waiting for the results of this review. If the internal review is finalised after 60 days, the applicant will have 28 days from the date they were notified of the result of the internal review to go to the Tribunal.

10. For complaints about a person’s health information go to Q.11 For complaints about a person’s personal information, not including health information, tick all of the following types of conduct that describe the complaint. Then go to Q.12.

☐ Collection of the complainant’s personal information (IPP 1-4)

☐ Security or storage of the complainant’s personal information (IPP 5)

☐ Refusal to let the complainant access or find out about their own personal information (IPP 6-7)

☐ Accuracy or relevance of the complainant’s personal information (IPP 8-9)

☐ Use of the complainant’s personal information (IPP 10)

☐ Disclosure of the complainant’s personal information (IPP 11-12, and/or the public register provisions in Part 6 of the Act)

☐ Other / it’s not clear

Note: ‘Conduct’ can include an action, a decision, or even inaction by your agency. For example the ‘conduct’ in this case might be a decision to refuse the complainant access to his or her personal information, or the action of disclosing his or her personal information to another person, or the inaction of a failure to protect the complainant’s personal information from being inappropriately accessed by someone else.

11. For complaints about a person’s health information, tick all of the following types of conduct which describe the complaint:

☐ Collection of the complainant’s health information (HPPs 1-4)

☐ Security or storage of the complainant’s health information (HPP 5)

☐ Refusal to let the complainant access or find out about their own health information (HPPs 6-7)
Accurary or relevance of the complainant’s health information (HPPs 8-9)

Use of the complainant’s health information (HPP 10)

Disclosure of the complainant’s health information (HPP 11)

Assignment of identifiers to the complainant (HPP 12)

Refusal to let the complainant remain anonymous when entering into a transaction with your agency (HPP 13)

Transfer of the complainant’s health information outside New South Wales (HPP 14)

Including the complainant’s health information in a health records linkage system (HPP 15) Other / it’s not clear

Note: See Q.14 on Privacy Complaint: Internal Review Application Form, if they have used that form. (It is not compulsory for the complainant to use any particular format, so long as their request is in writing.)

12. Insert the reviewing officer’s name here:

____________________ - __________________

Appoint a reviewing officer. (The reviewing officer must be someone who was not substantially involved in any matter relating to the conduct complained about. For other requirements see s.53(4) of the PPIP Act. This also applies to the HRIP Act.)

13. Write to the complainant, stating:

• your understanding of the conduct complained about;

• your understanding of the privacy principle/s at issue (either IPPs at Q.10 or HPPs at Q.11);

• that the agency is conducting an Internal Review under the PPIP Act or the HRIP Act, as appropriate;

• the name, title, and contact details of the reviewing officer;

• how the reviewing officer is independent of the person/s responsible for the alleged conduct;
• the estimated completion date for the review process;
• that if your review is not complete by the date at Q.9, the complainant can go to the Tribunal for an external review of the alleged conduct and the relevant time frame to apply for a Tribunal review; and
• that notice of your application and the subject matter of the application “s54 PPIP will be provided to the NSW Privacy Commissioner for their oversight role.

Note: s54 of the PPIP Act (s of HRIP) requires the agency to:

1. Notify the Privacy Commissioner that it has received the application

2. That it must inform the Privacy Commissioner of the progress of the internal review

3. Inform the Privacy Commissioner of the findings and action it proposes to take. As the Privacy Commissioner is entitled to make submissions.

14. Send notice of the application (s54 PPIP) at Q.13
to: NSW Privacy Commissioner
GPO Box 7011, SYDNEY NSW 2001

Or fax (02) 8114 3756
or email ipcinfo@ipc.nsw.gov.au

Include a copy of the complainant’s application – either the written request or the information provided on the Privacy

Complaint: Internal Review Application Form.

You can now start the review itself

15. a) Under the PPIP Act, you need to determine:
• whether the alleged conduct occurred;
• if so, whether the conduct complied with all the IPPS (and Part 6 public register provisions if applicable) and
• if the conduct did not comply with an IPP (or the public register provisions), whether the non-compliance was authorised by:
  - an exemption under the PPIP act,
  - a privacy code of practice, or
  - a s.41 Direction from the Privacy Commissioner b)
Under the HRIP Act, you need to determine:

• whether the alleged conduct occurred;
• if so, whether the conduct complied with all the HPPs, and
• if the conduct did not comply with an HPP, whether the non-compliance was authorised by:
  - an exemption under the HRIP act,
  - a health privacy code of practice, or
  - a s.62 Direction from the Privacy Commissioner.

16. It is recommended that four weeks after sending the notice that an application has been received at Q.13, you send a progress report to the Privacy Commissioner and (if required) the complainant, including:
• details of the progress of the review;
• if there are delays, you may wish to provide an explanation of this and a revised estimated completion date for the review process; and
• a reminder that if the review is not complete by the date at Q.9, the complainant can go to the Tribunal for an external review of the alleged conduct and the relevant timeframe to apply for a Tribunal review.

On completion of the review

17. a) Under the PPIP Act, you need to determine:
• whether the alleged conduct occurred;
• if so, whether the conduct complied with all the IPPs (and Part 6 public register provisions if applicable)[i]; and
• if the conduct did not comply with an IPP (or the public register provisions), whether the non-compliance was authorised by:
  - an exemption under the PPIP Act
  - a Privacy Code of Practice; or
  - a s.41 Direction from the Privacy Commissioner.
  - an appropriate action for the agency by way of response/remedy.

Notes: Don’t forget to look at all the IPPs, as they can be inter-related. For example a complaint about disclosure (IPPs 11 and 12 and the public register provisions) might also raise issues about data security under IPP 5, or notification about collection at IPP 3. Exemptions are found in the PPIP Act at sections 4-6, 20, and 23-28.

Privacy Codes of Practice are instruments made by the Attorney General (under the PPIP Act). Many can be found on the IPC website at: www.ipc.nsw.gov.au.

Section 41 Directions only modify the IPPs, not the public register provisions. These Directions are usually temporary so check the dates carefully, and contact IPC for earlier versions of Directions if necessary. View all current s.41 Public Interest Directions.

b) Under the HRIP Act, you need to determine:
• whether the alleged conduct occurred;
• if so, whether the conduct complied with all the HPPs; and
• if the conduct did not comply with an HPP, whether the non-compliance was authorised by:
  - an exemption under the HRIP Act;
  - a Health Privacy Code of Practice; or
  - a s.62 Direction from the Privacy Commissioner.
  - an appropriate action for the agency by way of response/remedy.

Notes: Don’t forget to look at all the HPPs, as they can be inter-related. For example a complaint about disclosure (HPP
11) might also raise issues about data security under HPP 5, or notification about
collection at HPP 4. Exemptions are found in the HRIP Act at sections 5, 10, 13-17,
22 and within the HPPs in Schedule 1.

Health Privacy Codes of Practice are instruments made by the Health Minister (under the HRIP Act). View the Privacy
Codes of Practice on the IPC website.

Section 62 Directions modify the HPPs. These Directions will usually be temporary so check the dates
carefully. Current section 62 Directions can be viewed on the IPC website.

18. Before completing the review, check whether the Privacy Commissioner wishes to make a
submission. Ideally you should provide a draft copy of your preliminary determination to the Privacy
Commissioner for comment. At the very least you are required to provide the Privacy
Commissioner with the findings of the review and the action your agency proposes to take
(sS4(1)(c)).

19. a) Under the PPIP Act, finalise your determination of the internal review, by making one of the
following findings:

• Insufficient evidence to suggest alleged conduct occurred
• Alleged conduct occurred but complied with the IPPs/public register provisions
• Alleged conduct occurred; did not comply with the IPPs/public register provisions; but
  non-compliance was authorised by an exemption, Code or s.41 Direction
• Alleged conduct occurred; the conduct did not comply with the IPPs/public register provisions; the
  non-compliance was not authorised (‘a breach’).

b) Under the HRIP Act, finalise your determination of the internal review, by making one of the
following findings:

• Insufficient evidence to suggest alleged conduct occurred
• Alleged conduct occurred but complied with the HPPs
• Alleged conduct occurred; did not comply with the HPPs; but non-compliance was authorised by an exemption, Code or s.62 Direction

• Alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised (‘a breach’).

20. a) Did the agency breach an IPP or public register provision?

☐ Yes - go to Q.22
☐ No - go to Q.21

b) Did the agency breach an HPP?

☐ Yes - go to Q.22
☐ No - go to Q.21

21. Even though the agency did not breach any IPP, public register provision or HPP, have you identified any need for improvement in policies, procedures, communicating with clients, etc?

☐ Yes – go to Q.22
☐ No – go to Q.24

22. What action is proposed by the agency as a result of this review? (You can have more than one)

☐ Apology to complainant
☐ Rectification to complainant, e.g.: Access to their personal information or health information
☐ Correction of their personal information or health information
☐ Other type of rectification
☐ Expenses paid to complainant
☐ Compensatory damages paid to complainant
☐ Other remedy to complainant
☐ Review of policies, practices or systems
☐ Change in policies, practices or systems
☐ Training (or further training) for staff
☐ Other action
☐ No Action

23. Is the proposed action likely to match the expectations of the complainant?

☐ Yes
24. a) Under the PPIP Act, notify the complainant and the Privacy Commissioner in writing:

- that you have completed the Internal Review;
- what your findings are, i.e. which one of the following:
  - insufficient evidence to suggest alleged conduct occurred
  - alleged conduct occurred but complied with the IPPs/public register provisions
  - alleged conduct occurred; did not comply with the IPPs/public register provisions; but non-compliance authorised by an exemption, Code or s.41 Direction
  - alleged conduct occurred; the conduct did not comply with the IPPs/public register provisions; the non-compliance was not authorised (‘a breach’)
- what the reasons for your findings are;
- a plain English explanation of the law behind your findings, including quoting in full the relevant legislative provisions you are talking about;
- what action/s you are going to take as a result;
- that the complainant has the right to apply to the Tribunal within 28 days¹ for a review of the conduct complained about; and
- the contact details for the Tribunal.

b) Under the HRIP Act, notify the complainant and the Privacy Commissioner in writing:

- that you have completed the Internal Review;
- what your findings are, i.e. which one of the following:
  - insufficient evidence to suggest alleged conduct occurred
  - alleged conduct occurred but complied with the HPPs
  - alleged conduct occurred; did not comply with the HPPs; but non-compliance authorised by an exemption, Code, or s.62 Direction
- alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised (‘a breach’)
- what the reasons for your findings are;
- a plain English explanation of the law behind your findings, including quoting in full the relevant legislative provisions you are talking about;
- what action/s you are going to take as a result;
- that the complainant has the right to apply to the Tribunal within 28 days² for a review of the conduct complained about, and
- the contact details for the Tribunal.

¹ 28 days from the date of the notice.
² 28 days from the date of the notice.
25. Keep a record of this review for your annual reporting requirements

For more information

Contact the Information and Privacy Commission NSW (IPC): Freecall:
1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au

1 Refer to Rule 24 of the Civil and Administrative Tribunal Rules 2014
2 Refer to Rule 24 of the Civil and Administrative Tribunal Rules 2014