MACQUARIE
University
SYDNEY·AUSTRALIA

PRIVACY MANAGEMENT PLAN

June 2017

CONTENTS

Section 1: OVERVIEW

1.1 Introduction

Macquarie University (**the University**) is about discovery, learning and participation in a borderless world. We are a dynamic, flexible and engaged university committed to excellence in research, teaching and global citizenship. In undertaking its learning and teaching, research, community engagement functions and provision of health and wellbeing services, the University collects, uses, discloses and holds a broad range of personal and health information relating to students (including prospective, current and alumni), staff, patients and third parties.

This information is entrusted to the University and the University is required under the *Privacy and Personal Information Protection Act (NSW) 1998* (**PPIPA**) and the *Health Records and Information Privacy Act (NSW) 2002* (**HRIPA**) (collectively the "**Privacy Acts**") to ensure its protection.

The University has developed this Privacy Management Plan (**Plan**) in accordance with section 33 of PPIPA. This Plan sets out the University's commitment to respecting the privacy rights of its students, staff, patients and third parties. It also explains the University's practices and procedures in handling personal information under PPIPA and health information under 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 Privacy Acts in the course of collecting, managing, using, disclosing and securing personal and health information.

1.2 What does this cover?

Personal Information

Definition

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

'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics...'

Personal information held by the University

The University collects and holds personal information to support its functions related to learning and teaching, research, student administration, student services and activities, complaints and disciplinary activities, recruitment and employment activities, health and well-being activities, employment and relationships with external parties for commercial, philanthropic and marketing purposes.

Personal information can be stored in a range of locations, forms and formats (for example, paper-based formats, digital 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).

The information collected includes the following and is stored in the following ways (this is not an exhaustive list):

	Students	Staff	External
Type	- Personal identifiers (e.g. names, student identification numbers, address, contact details) - Digital photos for student identification cards - Financial information (e.g. tax file numbers, HECS information, information relating to student loans) - Assessment information (including examiners' reports, practicum assessments, academic results)	- Personal identifiers (e.g. names, staff identification numbers, address, contact details) - Digital photos for staff identification cards - Financial information (e.g. tax file numbers, banking details, remuneration details, superannuation details) - Previous employment details - Staff communications	- Personal identifiers (e.g. names, contact details) of individuals associated with the University such as benefactors, sponsors, consultants, contractors, suppliers, users of the University's facilities etc. - Financial information (e.g. banking details of contractors, consultants, suppliers) - Some records of the University's governance bodies (particularly Council, and Senate and its subcommittees) may refer to personal information relating to external persons

	Students	Staff	External
Storage	- CRM systems (Student 1 and Tracker) hold student identifiers, enrolment, admission, and progression information - 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 learning management system (Moodle/iLearn) contains student identifiers, assessment records, communications between students and academic staff	- Human Resources electronic information management systems and staff files contain most staff information - ICT systems contain staff identifiers including staff email and other University accounts - The University's website and publications (including the publicly accessible staff directory) may provide staff identifiers including name, position, telephone number, office location, email address and qualifications	- Marketing systems hold information regarding benefactors and sponsors - Financial systems hold information about suppliers, vendors and contractors - Committees and governance bodies may hold personal information of external persons relevant to the performance of their relevant functions
	- The University Library holds records on students, staff and other users to identify users and facilitate Library privileges - University Security retain records relating to car parking permits, CCTV footage, and incident notifications and reports		

Some of the University's research and teaching activities involve the collection of data of people both inside and outside the University which may also include personal or health information (this may be held by the University or by individual researchers). Human-based research projects require prior approval by the University's Human Ethics Research Committee (HREC), and as part of this process, consent is normally obtained in respect of the collection, use and disclosure of personal or health information for research purposes. However, consent for research purposes may not be required in certain situations (see section 4.1 of this Plan).

Further information regarding research considerations can be obtained from the Privacy Toolkit.

Health Information

Definition

The HRIPA defines health information, in s 6, as

a) *Personal information that is information or an opinion about:*
   i. *the physical or mental health or a disability (at any time) of an individual; or*
   ii. *an individual's express wishes about the future provision of health services to him or her, or*
   iii. *a health service provided or to be provided to an individual; or*
b) *other personal information collected to provide, or in providing a health service, or*
c) *other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or*
d) *other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or*
e) *healthcare identifiers'*

Health information held by the University

The University collects and manages health information as a provider of certain health services and in relation to its training and education of health care professionals. This includes the University's medical and health service providers including the clinics, and Campus Wellbeing medical and counselling services. Health information of patients (including staff, students and others) is collected and used to enable these services to perform their functions including the education and training of health care professionals (e.g. information related to clinical practice undertaken by students).

The information collected includes the following and is stored in the following ways (not exhaustive):

	As a health service provider	As a public educational institution	As an employer
Type	- Medical records of patients receiving health services from any of the Clinics, counselling services etc.	- Student welfare information (e.g. health and medical information, disability and equity information) - Research involving the use of health information	- 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)
Storage	- Health record systems such as TrakCare	- CRM systems (Student 1 and Tracker) hold student medical information - Faculties, Departments, and individual staff members will also hold research information	- Human Resources electronic information management systems and staff files contain most staff information

Exclusions

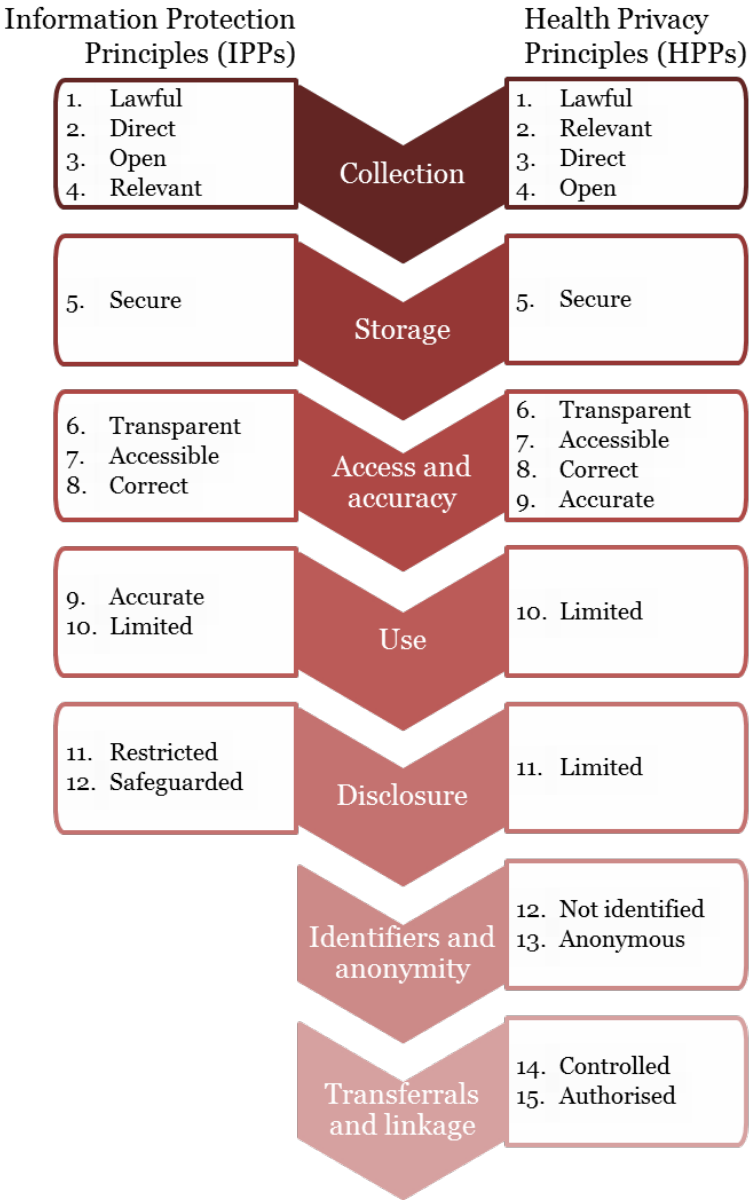
The following are some relevant examples of categories of information that are excluded from the scope of both the PPIPA and HRIPA:

- Information about an individual who has been dead for more than 30 years
- Information about an individual that is contained in a publicly available publication
    - 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
- Information or an opinion about an individual's suitability for appointment or employment as a public-sector official

A full list can be found within the legislation.

1.3 What are the University's responsibilities?

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 information, with the HRIPA additionally covering identifiers and anonymity as well as transferrals and linkage. This is detailed below:



These are the legal obligations which the University must abide by when collecting, storing, using or disclosing personal and health information. Some exemptions do apply which are detailed in Section 4.1.

Further detail on how the University is meeting these obligations is included in Section 2 of this document.

1.4 Further information

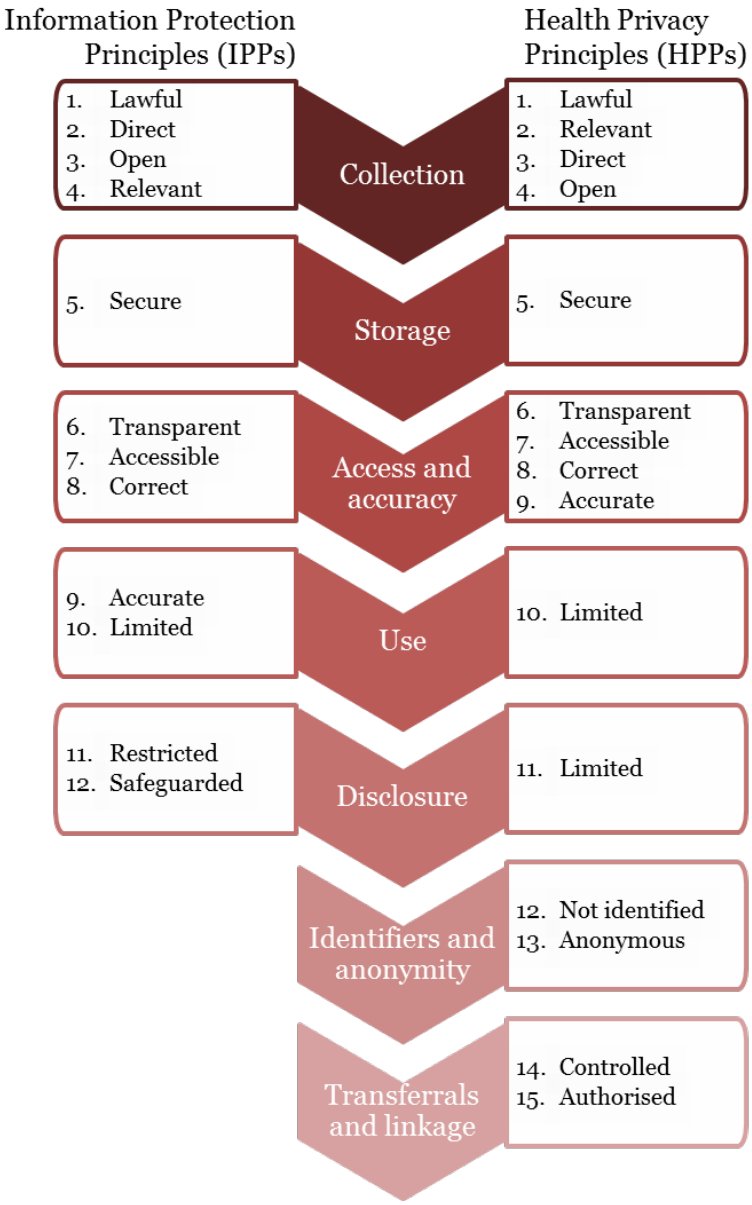
Further guidance is set out in the following sections of this Plan as follows:

- Applying the principles
- Complaints and breaches
- Other information
- Training and support

Additional resources including all relevant forms and templates, and accompanying policies and procedures can be found in the Privacy Toolkit or by contacting the Privacy Officer, via email at privacyofficer@mq.edu.au, or phone on (02) 9850 4587.

Section 2: APPLYING THE PRINCIPLES

2.1 The Information Protection Principles (IPPs) and Health Privacy Principles (HPPs)



How the University complies with the IPPs and HPPs is set out below. Where there is overlap between the IPPs and HPPs these have been addressed as one.

2.2 Collection

IPP 1 / HPP 1 – Lawful

An agency must only collect personal and health information for a lawful purpose. It must be directly related to the agency's function or activities and necessary for that purpose.

Personal and health information must only be collected by lawful means, for a lawful purpose, directly related to a function or activity of the University, and reasonably necessary for that purpose.

These purposes include, primarily, functions relating to admission, enrolment, progression, and graduation of students (including teaching); communication with prospective students and alumni; student activities; medical and health services; recruitment, selection, appointment, management, and payment of staff; research; and business dealings that support the functions of the University.

An example of the collection principle as it relates to both personal and health information is:

1. A student registers for counselling services provided by the University
2. The counselling service obtains both personal and health information from the student to perform its function of providing counselling services
3. The counselling service can only obtain personal and health information from the student
    1. by lawful means (i.e. from student or from other health professionals with student's permission) and
    2. for lawful purposes (i.e. providing counselling services or any other service directly related and necessary to provision of counselling services)

IPP 2 / HPP 3 – Direct

IPP2 - An agency must only collect personal information directly from the individual, unless the individual has authorised collection from someone else, or if the information relates to a person under age of 16, it has been provided by a parent or guardian.

HPP3 – An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

Wherever possible, the University must collect personal and health information directly from the individual the information relates to subject to the above exemptions. 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
- Students / staff can authorise the University to collect health information from their medical or health practitioners
- parents of children under 16 can provide this information on behalf of their children.

The University is not required to comply with IPP 2 / HPP3 if the information concerned is collected in connection with proceedings (whether or not actually commenced) before any court or tribunal.

IPP 3 / HPP 4 – Open

Before or as soon as practicable after collection, an agency must inform an individual that the information is being collected, why it is being collected, who will receive it, how it will be used, and to whom it may be disclosed. Individuals must also be told how they can access and correct their personal and health information, if the information is required by law or is voluntary, and any consequences that may apply if they decide not to provide it.

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 following:

- The identity of the party collecting the information and how to contact it
- The reason for the collection of the information
- The parties to whom the information is usually disclosed to
- How the individual can access and correct the information being collected, and
- The consequences that may apply if the individual decides not to provide that information

The University informs individuals of the above matters through its collection notices (available on the University's Privacy webpages), privacy statements and consent forms as required. Consent is a key control to ensure the individual has understood and provided informed consent.

Where the supply of information is voluntary (i.e. it is not required by law), the University explains (in its collection notices) 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 seeking counselling or health services, the University explains that it cannot provide those services without certain personal and health information being provided.

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

IPP 4 / HPP 2– Relevant

An agency must ensure that personal and health information is relevant, accurate, complete, up-to-date and not excessive. The collection should not unreasonably intrude into personal affairs.

When deciding to collect personal and / or health information, the University must consider the relevance, necessity, and accuracy of the information, and take care not to intrude on the personal affairs of individuals from whom information is being sought.

For example, students submitting Disruption to Studies notifications are asked to provide documentary evidence of the nature of the disruption, the dates and / or length of the disruption, the severity and impact of the disruption on their ability to complete an assessment, and whether the disruption relates to a pre-existing condition.

The student is only requested to provide information that is relevant to their disruption of study notification.

2.3 Storage

IPP 5 / HPP 5 – Secure

An agency must store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also take reasonable security safeguards to protect personal information from unauthorised access, use, modification or disclosure.

The security of personal information collected by the University is paramount, 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, use and disclosure.

Digital Information Security

Information security is fundamental to information privacy. The University recognizes the fast moving pace of IT security technological advances and the sophistication of security attacks. As such, the University has a strategic focus to mature and reinforce the security and integrity over information and data. To this end, relevant Information Security Policies and Procedures are reviewed and refreshed on an ongoing basis to ensure their effectiveness. In accordance with the Information Security Policy a number of key controls are in place to ensure the protection of personal information some of which have been included below:

- Governance
    - Direction and support for information security is driven by the Chief Information Officer and Macquarie IT Senior Leadership Team. Appropriate policies and procedures have been put in place to ensure that relevant governance structures are in place.

- Information security systems
    - Security software has been deployed across Macquarie University's computing systems and network components
    - The University's information security management practices apply the international standard ISO/IEC 27001:2013 and the information security systems are maintained and continually improved with this standard in mind

- Information classification labelling and handling
    - All university data that is stored, processed, or transmitted on university IT resources (or on other IT resources where university business occurs) are classified into one of three categories.
        - Confidential
        - Controlled
        - Published

      Minimum standards have been developed that should be applied to Confidential, Controlled and Published data categories to ensure it receives the appropriate level of protection and comply with the relevant laws and regulations.

- Security considerations are also taken into account in arrangements for data transmission (including encryption and password protection where appropriate), backup and storage.

- Controlling access to information systems
  - Systems provide secure storage for confidential data as required by confidentiality, integrity, and availability needs. Security is provided by firewall controls, encryption access controls, file system audits, physically securing the storage media, or any combination or other means deemed appropriate.
  - Formal procedures are in place to control the allocation of access rights to information systems and services. These procedures cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.
  - The University monitors IT Resources by performing the following system audits:
    - reviewing privileged access quarterly, to ensure continued access is required
    - logging and auditing use of and changes to IT systems and services, and
    - retaining security logs for monitoring and investigations.
  - Passwords are required when using work computers, portable devices and email communications to meet the policy requirements, including conforming to strength requirements.

- Acquisition, development and maintenance of information systems and services
  - To maintain the security of application system software and information the following have been implemented:
    - Change control procedures
    - Technical review of applications after operating system changes
    - Restrictions on changes to software packages
    - Supervision and monitoring of outsourced software development

- Relationships with external third parties and information disclosed outside NSW or to Commonwealth agencies
  - Where it is necessary for personal or health information to be disclosed to a third party provider, such as the University Admissions Centre (UAC), for the purposes of providing a service, the University ensures that appropriate contractual protections are included in the contract with the provider to prevent unauthorised use or disclosure of personal or health information.
  - Contracts with third party providers include appropriate standards for data protection and require compliance with the relevant privacy principles.
  - Where the University intends to disclose personal or health information to a third party service provider outside of NSW or to a Commonwealth agency, the University takes reasonable steps to ensure that the information it has disclosed will not be held, used or disclosed by the recipient inconsistently with the IPPs / HPPs. It does this by:
    - including contractual protections requiring the recipient to comply with the IPPs / HPPs and the Privacy Commissioner's guidance on transborder disclosures;

        - making an assessment to determine that the privacy protections operating in the destination jurisdiction are substantially similar to those in NSW; and
        - conducting audits over the service providers' IT systems before the contract is entered into and during the term of the contract.

- Training and awareness
    - Information security awareness training activities are conducted periodically for the University's staff and students.
    - University Staff are advised of new or updated policies and procedures through the intranet and, on occasion, targeted training.

- Breaches/Disciplinary Action
    - The University has comprehensive policies, procedures and processes in place to appropriately respond to data security breaches. This includes procedures to ensure that security events (possible or potential breach or failure of safeguards) and security incidents are reported, investigated and properly managed.
    - The University also has log monitoring tools in place which help detect unauthorised access and use of our systems. For example, attempts to bypass access controls will be detected by the log monitoring tools and relevant staff alerted.
    - The University has policies and procedures in place to investigate and take appropriate disciplinary action against University staff found responsible for data breaches.

Records Management

The University's records are governed by the State Records Act 1998 (NSW) and associated Standard on Records Management issued by the State Archives & Records Authority of NSW. The University's record management system has been identified as a secure and authoritative repository for the University's digital record storage and management. It ensures that the following controls are in place to ensure information security and accuracy:

- Version Control
- Access Control
- Unique ID
- Audit Log

The University keeps information for only as long as necessary or as required by law, reducing the risk that it may be mishandled. If we find that we have no further need for your personal information we may archive it in accordance with our record retention obligations or securely destroy all record of it in a secure manner as appropriate (for example, using secure (locked) recycling bins and shredders).

2.4 Access & Accuracy

IPP 6 / HPP 6 – Transparent

An agency must provide an individual with details regarding the personal and health information they are storing, why they are storing it and what rights individuals have to access it.

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 the information being held
- the main 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 it if it is not accurate

IPP 7 / HPP 7 – Accessible

An agency must allow access to personal and health information without excessive delay or expense.

Students can view their information collected as part of the admission and enrolment process via eStudent, or by contacting Ask MQ. Staff can contact HR to request their information or use HROnline to see what personal information is currently stored. Patients of University counselling and other health and clinic services can contact the service directly.

All requests for access should follow the Request for Information process. The University will allow any individual to access the information held about them in accordance with the PPIPA and HRIPA, in most cases at no cost and through an informal request process. Applications for access will be processed in a timely fashion.

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

IPP 8 / HPP 8 – Correct

An agency must allow an individual to update, correct or amend personal and health information where necessary.

Students can update their information collected as part of the admission and enrolment process via eStudent, or by contacting Ask MQ. Staff can contact HR to correct or update some of their information in HROnline. Patients of University counselling and other health services can update their records by contacting the service directly.

If any other changes are required a written request can be made through the Application for Changes to be made to Personal Information Form.

2.5 Use

IPP 9 / HPP 9 – Accurate

An agency must ensure that personal and health information is relevant, accurate, up to date and complete before using it

The University must take reasonable steps to ensure that the information it holds is relevant, accurate, up to date, and not misleading, having regard to the purpose(s) for which the information is to be used. The preference of the University is to have one authoritative source of information that can be maintained as opposed to multiple sources which risk being incomplete, inconsistent or outdated.

Additionally, staff and students can update certain information themselves, such as contact details, through the available IT systems.

Prior to using personal information, the University will take reasonable steps to check its accuracy by taking the following into consideration:

- What was the purpose for which the information was collected?
- When was it collected?
- What was the context in which this information was collected?
- What purpose is the information going to be used for?
- Who has access to this information? And who has access to edit this information?
- How important is the accuracy of this information?
- What is the impact on the individual if the information is inaccurate, out-of-date or irrelevant?
- Is it possible to correct inaccuracies prior to use?
- What are the barriers to checking the information? e.g. effort and cost

The University will not use personal or health information where it is known to contain erroneous information.

IPP 10 / HPP 10 – Limited

The use of personal and health information held by the University is limited to the primary purpose(s) for which it was collected, unless an exemption applies.

Under the PPIPA, an agency can only use "personal" information for the purpose for which it was collected (primary purpose) unless:

- an individual has given consent, or
- the use for the secondary purpose is directly related to the primary purpose, or
- the use for a secondary purpose is necessary to prevent or lessen a serious or imminent threat to any person's life or health.

Under the HRIPA, the University can only use "health" information for a secondary purpose if an exemption applies including any of the following:

- if the secondary purpose is directly related to the primary purpose for which the information was collected,
- to prevent or lessen a serious and imminent threat to the life, health or safety of a person,
- where it is reasonably necessary for law enforcement purposes or for the protection of public revenue,
- where unlawful activities have been or may be engaged in,
- where an employee may have engaged in conduct that may be grounds for disciplinary action, or
- for the exercise of complaint handling functions or investigative functions by investigative agencies.

More exemptions of use of health information for secondary purposes are set out in HPP 10.

The general uses of personal and health information collected by the University are set out in the University's privacy collection notices (e.g. Enrolment, Admissions, Employment etc.). Consent forms are used where the collection of information is health information or the proposed use of the information is outside the "uses" contemplated by the standard privacy collection notices.

The University takes reasonable steps to ensure that personal and health 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 of the University that did not undertake the initial collection of the information, if this is for the same purpose, directly related to a purpose for which it was originally collected or otherwise falls under an exemption.

2.6 Disclosure

IPP 11 – Restricted / HPP 11 - Limited

An agency can only disclose personal and health information for secondary purposes in limited circumstances as set out in the Privacy Acts.

Under the PPIPA, the University can disclose personal information for a secondary purpose if

- the individual consented, or
- the secondary purpose is directly related to the primary purpose and the University reasonably believed the individual would not object to the disclosure, or
- the agency reasonably believes on reasonable grounds the disclosure is necessary to prevent a serious and imminent threat to any person's life, health or safety.

In addition to the above, the University cannot disclose an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities ("**personal sensitive information**") unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of any individual.

The University does not disclose "personal information" it holds about students, alumni, staff, or members of the public to external third parties for secondary purposes unless it falls within one of the above exemptions or the University is authorised or required by law.

For example, where the University offers academic or research programs in conjunction with another academic or research institution, it may need to exchange personal information with these institutions in order to facilitate student enrolment and progression through the program. This would be a secondary purpose that is directly related to the primary purpose and the University reasonably believed the individual would not object to the disclosure.

Under the HRIPA, the University can disclose an individuals' health information for a secondary purpose if:

- the individual has consented, or
- the secondary purpose is directly related to the primary purpose for which the information was collected, and the individual would reasonably expect the University to disclose that information for a secondary purpose, or
- 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, or
- the University believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life, health or safety of a person or a serious threat to public health or safety, or
- the University has reasonable grounds to suspect an unlawful activity has been or may be engaged in, or
- necessary for the exercise of law enforcement functions by law enforcement agencies, or
- necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

- the disclosure is permitted by a Public Interest Direction made by the NSW Privacy Commissioner (see section 1.3 of this Plan)

An example of secondary purpose is if information is collected to provide a health service to the individual, and that health information is disclosed to another health service provider (providing services to that individual) then that is a disclosure for a secondary purpose directly related to the primary purpose and is permitted. More exemptions are set out in HRIP 11.

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 to law enforcement agencies in relation to law enforcement, for example:

- 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

Restrictions on Transborder Disclosures

In addition to the normal disclosure rules, the University will not disclose (or transfer) personal or health information to any person or body outside NSW or to a Commonwealth agency (**transborder disclosure**) unless one of the following exemptions apply:

- the other party is subject to a law, scheme or contract that upholds principles substantially similar to the information privacy principles
- the individual concerned has consented
- the transfer is necessary for the performance of a contract between the individual and the University or the University and a third party
- the transfer will benefit the individual concerned, but it is impracticable to obtain their consent, and if notified would likely consent
- the disclosure is reasonably believed by the University to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person
- the University has taken reasonable steps to ensure the information won't be dealt with inconsistently with the information privacy principles (e.g. we have bound the recipient by contract to privacy obligations equivalent to the principles), or
- if it is permitted by any other exemption in the Privacy legislation, permitted or required by any Act or any other law

Where information is disclosed transborder, the University will make an assessment to determine that the privacy protections operating in the destination jurisdiction are substantially similar to those in NSW and put in place contractual terms to ensure the protection of the information provided.

IPP 12 – Safeguarded

*Under the PPIP Act, an agency cannot disclose personal information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership (**personal sensitive information**) without consent. It can only disclose personal sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.*

There are stricter obligations for the disclosure of personal sensitive information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health, and sexual activities. The University will not disclose this information unless it is reasonably necessary for law enforcement purposes, is required by law or if the disclosure is necessary to prevent a serious or imminent threat to the life or health of a person.

The same restrictions on transborder disclosures apply to this type of information.

2.7 Identifiers and anonymity

HPP 12 – Not identified

An agency must only identify people by using unique identifiers if it is reasonably necessary to carry out the agency's functions efficiently.

An identifier is defined in section 4 of the HRIPA to mean something that an organisation assigns to a person in order to uniquely identify that person (usually a number). The identifier will have either been created, adopted, used or disclosed in conjunction with or in relation to the person's health information. A person's name is not an identifier.

The University assigns unique identifiers for the purpose of patient identification. This is necessary in the University's capacity as a Health Care Service Provider for the identification of patients and their treatments. It is acknowledged that these identifiers are classified as health information and are subject to the HRIPA and protected as such.

HPP 13 – Anonymous

An agency must give an individual the option of receiving services anonymously, where this is lawful and practicable.

Wherever it is lawful and practicable, the University will give people the opportunity to remain anonymous when entering into transactions with, or receiving health services from, the University.

However, in the context of providing health services it is generally impracticable to transact with an individual anonymously due to the type of information required from an individual, such as:

- personal contact details
- Medicare details and private health insurance information being required to complete the transaction
- previous medical history, referrals etc.
- ongoing health care requiring follow-up
- bank account / credit card details

Accordingly, it will be impossible to provide health services to individuals anonymously in this context.

2.8 Transferrals and linkage

HPP 14 – Controlled

In addition to the normal disclosure rules under HPP11 of HRIPA, the same disclosure restrictions (Transborder flows and Commonwealth agencies) apply to health information (see section 2.6 above).

HPP 15 – Authorised

An agency must not include health information or disclose an individual's identifier for inclusion in health information in a health records linkage system unless the individual has provided their express consent.

A "health records linkage system" means a computerised system designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records.

Consent is not required if:

- the University is lawfully authorised or required not to obtain consent.
- non-compliance is otherwise permitted (or necessarily implied or contemplated) under an Act or other law (including the *State Records Act 1998*); or
- the inclusion of health information about the individual in the health records linkage system is a "use" of the information that complies with HPP10(1) (f) or a disclosure that complies with HPP 11 (1) (f).

HPP10(1) (f) permits the "use" of health information for the secondary purpose of conducting research, or compilation or analysis of statistics in the public interest if certain conditions are satisfied.

HPP 11 (1) (f) permits the "disclosure" of health information for the secondary purpose of conducting research, or compilation or analysis of statistics in the public interest if certain conditions are satisfied.

The University only uses health records linkage systems (such as My Health Record) when individuals have expressly consented to their information being included on such a system unless one of above the exemptions apply.

Section 3: COMPLAINTS AND BREACHES

3.1 Complaints

The University is committed to protecting the privacy of personal and health information of students and staff in accordance with the privacy legislation.

How do I make a complaint?

If you think your privacy has been breached, you can make a complaint in one of the following ways:

- Contact the unit involved and resolve the matter informally
- Contact the Privacy Officer at privacyofficer@mq.edu.au
- Apply for an internal review (see section 3.2 below)
- Contact the Privacy Commissioner (see section 5.3 below)

3.2 Internal reviews

Who can request an internal review?

Any student or staff member who believes the University has misused their personal or health information can lodge an application for an internal review.

The University will conduct an internal review to determine:

- whether or not the alleged conduct occurred,
- if so, whether the University complied with its privacy obligations,
- if not, whether non-compliance was authorised by an exemption, Privacy Codes of Practice, a direction from the Privacy Commissioner or an appropriate action by way of a response / remedy

Once it completes its internal review, the University will advise you and the Privacy Commissioner of its findings and what it will do as a result.

Is there a time limit for lodging a request for an internal review?

Yes

The request for an internal review must be made within 6 months of the time:

- you became aware of the conduct, the subject of the complaint, or
- when you became aware of their rights under the Privacy legislation, or
- such later time as the University in its discretion may allow.

What is the process?

1. Formal complaints / applications for review must be made in writing, using the Internal Review Request Form.

2. When the University receives the written application for internal 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 was not substantially involved in any matter relating to the conduct which gave rise to the complaint and who is otherwise suitably qualified to deal with the matters raised in the application.

3. The internal review will be conducted in accordance with the Internal Review Checklist available in the Privacy Toolbox and the guidelines provided by the NSW Information and Privacy Commissioner. This will include:

    a. Interviews with key parties involved or identified in the application
    b. Consideration of:
        i. all relevant material submitted by the applicant
        ii. information obtained through interviews with relevant individuals
        iii. information obtained from the University's information and recordkeeping systems, policies and procedures or other relevant documents, and
        iv. relevant case law and NSW Civil and Administrative Tribunal decisions.

4. The outcomes of an internal review may include one or more of the following findings (this is not an exhaustive list):

    a. Insufficient evidence to prove alleged conduct occurred
    b. Alleged conduct did not occur, therefore no further action to be taken
    c. Alleged conduct occurred but complied with the IPPs / HPPs
    d. Alleged conduct occurred, conduct did not comply with the IPPs / HPPs but non-compliance was authorised
    e. Alleged conduct occurred, conduct did not comply with the IPPs / HPPs and non-compliance was not authorised (i.e. breach)
    f. Review / change in policies, practices or system controls to prevent recurrence of a breach, or undertake actions to prevent the conduct from recurring
    g. formal apology to the applicant
    h. training for staff
    i. appropriate remedial action as the University thinks appropriate
    j. undertakings that the conduct will not occur again

5. The draft findings of an internal review will be submitted by the reviewing officer to the Chief Operating Officer (or delegate), who is responsible for finalising the review. This may include approving any resulting recommendations.

6. Once approved, the draft report (including findings and recommendations) will be submitted to the Privacy Commissioner for comment before being finalised and sent to the complainant

7. Internal reviews will be completed within 60 days of the receipt of a formal application for review. The complainant and the Privacy Commissioner will be informed of the outcome of the review within the required timeframe unless notified otherwise.

What happens if the review is not completed within 60 days or if I am not happy with the result?

1. If the review is not completed within 60 days from the date the application was received or the complainant is dissatisfied with the University's findings, then the complainant has 28 days to make an application under section 55 to the NSW Civil and Administrative Tribunal (NCAT) for a review of the conduct or decision complained about.

2. If the internal review is finalised after 60 days, then the complainant will have 28 days from the date they were notified of the result of the internal review to go to the Tribunal.

The role of the Privacy Commissioner in internal reviews

The NSW Privacy Commissioner has an oversight role in the internal review process and may make submissions on internal reviews.

The University is required under the Privacy legislation to notify the Privacy Commissioner regarding the following:

- formal complaints received
- progress on internal reviews being undertaken, and
- findings of the reviews undertaken and the action proposed to be taken by the University.

The Privacy Commissioner is entitled to make submissions to the University with respect to the findings of the internal review and may at the request of the University undertake the internal review on behalf of the University.

3.3 External reviews

The only external review mechanism available under the PPIPA is the right to apply for an administrative review of the conduct or decision complained about to the NSW Civil and Administrative Tribunal (NCAT) when:

- an applicant is dissatisfied with the findings of an internal review or
- the University has not completed an internal review within 60 days of the application date.

The Role of NCAT

NCAT may order the University to change its practices, apologise or take steps to remedy any damage. NCAT may also award compensation if warranted.

NCAT's Contact Details

NCAT can be contacted as follows:

Office: NSW Civil and Administrative Tribunal, Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000
Postal: NSW Civil and Administrative Tribunal, PO Box K1026, Haymarket NSW 1240

Telephone: 1300 006 228

Website: www.ncat.gov.au

If the applicant is not satisfied with the determination of the NCAT, they have a right of appeal to the Appeal Panel of the NCAT.

3.4 Lodging complaint with Privacy Commissioner

A person aggrieved by the conduct of the University may complain directly to the NSW Privacy Commissioner, not as an external review mechanism, but as a complaint.

In this instance, the Privacy Commissioner may conduct a preliminary assessment of a complaint before deciding whether to deal with the complaint.

The Privacy Commissioner must inform the complainant of the internal review process available under Part 5 of PPIPA and may decide not to deal with the complaint if satisfied that:

a) the complaint is frivolous, vexatious or lacking in substance or not in good faith, or
b) the subject matter of the complaint is trivial, or
c) the subject matter of the complaint relates to a matter permitted or required by or under any law, or
d) there is available to the complainant an alternative, satisfactory and readily means of redress, or
e) it would be more appropriate for the complainant to make an application for an internal review under section 53.

If the Privacy Commissioner does decide to deal with the complaint, it must endeavour to resolve the complaint by conciliation.

The Privacy Commissioner may refer a complaint made to it to another person or body for investigation or other action, if considered appropriate.

When the NSW Privacy Commissioner deals with the complaints against the University, the Privacy Commissioner does not have determinative powers (i.e. the Privacy Commissioner cannot set aside or vary the decision of the University or award compensation).

Section 4: OTHER INFORMATION

4.1 Exemptions from IPPs / HPPs

Under s41 of PPIPA and s62 of HRIPA, 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.

Research Exemptions

PPIPA - Section 27B and Statutory Guidelines

The University may collect, use and disclose **Personal** Information for research purposes without obtaining an individual's consent provided it complies with all the criteria set out in section 27B of PPIPA, any Statutory Guidelines issued by the Privacy Commissioner and obtains approval of the University's Human Research Ethics Committee.

HRIPA - HPP10 (1) (f) and 11 (1) (f) and Statutory Guidelines

The University may collect, use and disclose **Health** Information for research purposes without obtaining an individual's consent provided it complies with all the conditions set out in HPP10(1)(f) and HPP11 (1)(f) of HRIPA, any Statutory Guidelines issued by the Privacy Commissioner and obtains approval of the University's Human Research Ethics Committee.

4.2 Offences

Part 8 of the PPIPA and HRIPA details offences for certain conduct. A table detailing the relevant penalties and associated provision has been provided below.

Offence	Maximum penalty	Legislative provision
It is a criminal offence for a public sector official to corruptly disclose and use personal or health information	• Fine of up to 100 penalty units ($11,000), or • Imprisonment for two years, or both	• s 62 of PPIPA • s 68 of HRIPA
It is a criminal offence for a person to offer to supply personal or health information that has been disclosed unlawfully	• Fine of up to 100 penalty units ($11,000), or • Imprisonment for two years, or both	• s63 of PPIPA • s69 of HRIPA
It is a criminal offence for a person – by threat, intimidation or misrepresentation – to persuade or attempt to persuade an individual: • to refrain from making or pursuing a request to access health information, a complaint to the Privacy Commissioner or the NSW Civil and Administrative Tribunal, or an application for an internal review; or • to withdraw such a request, complaint or application.	• Fine of up to 100 penalty units ($11,000)	• s 70(1) of HRIPA
A person must not – by threat, intimidation or misrepresentation – require another person to give consent under HRIPA, or require a person to do, without consent, an act for which consent is required.	• Fine of up to 100 penalty units ($11,000)	• s 70(2) of HRIPA
It is a criminal offence for a person to: • wilfully obstruct, hinder or resist the Privacy • Commissioner or a member of the staff of the Privacy Commissioner • refuse or wilfully fail to comply with any lawful requirement of the Privacy Commissioner or a member of the staff of the Privacy Commissioner, or • wilfully make any false statement to or mislead, or attempt to mislead, the Privacy Commissioner or a member of the staff of the Privacy Commissioner • in the exercise of their functions under PPIPA or any other Act	• Fine of up to 10 penalty units ($1,100)	• s 68(1) of PPIPA

In addition to the above, under section 308H of the Crimes Act, it is an offence to access or modify restricted data held in a computer where authorisation has not been provided. The maximum penalty being 2 years' imprisonment.

4.3 Linked legislation

Commonwealth Privacy Act 1988

The University is not required to comply with the Australian Privacy Principles in the Privacy Act 1988 (Cth) (**Privacy Act**) as it is not an 'organisation' within the meaning of the Act.

However, the University is a 'file number recipient' for the purposes of the Privacy Act because it holds records of employees and students 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 that are considered "organisations" are subject to the Privacy Act. For those entities affected refer to Appendix A.

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 in addition to the requirements under the Privacy Act. Additional requirements to comply with the Privacy Act have been detailed within the Privacy Toolkit for those controlled entities affected.

Government Information (Public Access) Act, 2009

The operation of the *Government Information (Public Access) Act* 2009 is not affected by the operation of PPIPA and HRIPA.

Note that GIPA provides access to various documents held by the University to any person subject to the operation of various exemptions in that Act. Under PPIPA and HRIPA access to information is provided only to the person to whom the information relates.

State Records Act 1998 (NSW)

The University is required to comply with the NSW *State Records Act* and associated Standard on Records Management issued by the State Archives & Records Authority of NSW. The provisions within the *State Records Act* provide overall guidance on the practical requirements for effective records and information management including retention periods and disposal of records and should be considered in conjunction with the Privacy Acts.

4.4 Key Related Policies and Procedures

The following University policies and procedures are related to the University's information handling practices:

- University Privacy Policy
- Information Security Policy
- Information Security Procedure
- Data Classification Procedure and Standards
- Records and Information Management Policy
- Records and Information Access and Security Procedure
- Records and Information Retention and Disposal Procedure
- Right to Information at Macquarie
- CCTV Policy, and
- Workplace Surveillance Policy

4.5 Public register

A public register is an official list of names, events and transactions. Under law, it is required to be available to the public.

The University does not maintain any public registers for the purposes of PPIPA or HRIPA, however some information is publicly available through University publications, such as staff details, and graduation records.

4.6 CCTV

The University also installs and maintains closed circuit television (CCTV) cameras on University premises for a number of purposes, including:

- to ensure the safety and security of staff, students and visitors whilst on University premises
- to protect assets and property of the University and others
- to assist in crime prevention and aid in the investigation of criminal activity or other misconduct, and
- to assist the University to manage its facilities, such as its car parks, computer labs and eating areas.

Prominent signage notifies all University students, employees, contractors and members of the public of the use of CCTV and that they may be under camera surveillance. The cameras are clearly visible. The operation of CCTV cameras as well as the monitoring and storage of CCTV images at the University only takes place in a centralised area within the University security office. Access to the CCTV images is controlled to ensure that only authorised personnel have access.

The installation, use and monitoring of CCTV cameras, including the storage, retention, use and disclosure of footage, is governed by the University's Closed Circuit Television (CCTV) and Workplace Surveillance Policy. This Policy was developed taking into account the guidelines provided by the *NSW Government policy statement and guidelines for the establishment and implementation of closed circuit television (CCTV) in public places.*

Section 5: TRAINING AND SUPPORT

5.1 Privacy Toolkit

The University's Privacy Management Plan is supplemented by a suite of tools within the Privacy Toolkit 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.

Included within this toolkit are forms and checklists that assist in the day to day operation of privacy. This toolkit provides best practice guidance and practical advice on matters including, but not limited to:

- Collection Notices
- Consent forms
- Internal review request forms and checklists
- How to request access to information
- How to correct, update or amend information

Links to associated policies and procedures are also included. The development and revision of policies and procedures is performed in consultation with the Privacy Officer to ensure that any impacts from the PPIPA and HRIPA are included. Any new policy or procedure, or any policy that is significantly changed or updated, is developed in consultation with relevant business areas and receives the endorsement of senior management and the Chief Operating Officer, before being circulated to staff. Policies and procedures, including this plan, are communicated to staff in a range of ways, including through our intranet, staff newsletters, induction of new staff and on-the-job training. Information about our privacy practices are also made available on our dedicated privacy page on our website.

5.2 Staff Training and Education

The University also provides regular training and education seminars to staff to inform them of their responsibilities under the Privacy Acts. Privacy news and updates are communicated to all staff on a regular basis.

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 or health information is being collected, used or disclosed for a lawful purpose
- if that lawful purpose is directly related to a function of the University or a secondary purpose
- whether or not the collection of that personal information is reasonably necessary for the specified purpose,
- whether any exemptions apply,
- how to make a complaint or request an internal review
- internal review process.

5.3 Public Awareness

The University promotes public awareness of the privacy obligations by:

- publishing this plan publicly on the University website
- publishing all policies, collection notices and privacy statements on the University website
- maintaining a dedicated privacy page for all privacy resources and contacts
- providing a dedicated privacy officer to manage privacy related issues / complaints / investigations
- making students, staff members and members of the public aware of the privacy obligations when completing forms that collect personal and health information.

Where the public has additional questions, they are encouraged to contact the Privacy Officer at privacyofficer@mq.edu.au or the Privacy Commissioner as below:

Office: Level 17, 201 Elizabeth Street, Sydney 2000
Postal address: GPO Box 7011, Sydney NSW 2001
Email: ipcinfo@ipc.nsw.gov.au
Tel: 1800 472 679