Privacy Management Plan

July 2019 | Version: 1

Contents

1 Introduction 4

1.1 Purpose 4

1.2 Scope 4

1.3 About Us 4

1.4 The Information and Health Principles 4

1.5 What is personal information? 5

1.5.1 What is not personal information? 5

1.6 What is health information? 5

1.6.1 What is not health information? 5

2 Personal and health information held by us 6

2.1 Types of personal and health information held by us 6

3 How we manage personal and health information 7

3.1 Introduction 7

3.2 Collection 7

3.2.1 Collection for lawful purposes (IPP 1 & HPP 1) 7

3.2.2 Direct collection (IPP 2 & HPP 3) 7

3.2.3 Requirements when collecting information (IPP 3 & HPP 4) 8

3.2.4 Relevant (IPP 4 & HPP 2) 8

3.3 Retention and security (IPP 5 & HPP 5) 9

3.4 Accuracy and access 10

3.4.1 Transparency (IPP 6 & HPP 6) 10

3.4.2 Access to personal and health information (IPP 7 & HPP 7) 10

3.4.3 Alterations to personal and health information (IPP 8 & HPP 8) 10

3.5 Use 11

3.5.1 Accuracy (IPP 9 & HPP 9) 11

3.5.2 Limited Use (IPP 10 & HPP 10) 11

3.6 Disclosure 12

3.6.1 Disclosure (IPPs 11 & 12 and HPPs 11 & 14) 12

3.6.2 Identifiers (HPP 12) 12

3.6.3 Anonymity (HPP 13) 12

3.6.4 Linkage of Health Records (HPP 15) 13

3.7 Exemptions to how we manage personal and health information 13

3.7.1 Specific exemptions contained in PPIPA and HRIPA 13

3.8 Offences 13

4 Strategies for compliance and best practice 13
4.1 Introduction 13
4.2 Policies and procedures 13
4.3 Promoting privacy awareness 14
4.4 Review and continuous improvement 14
5 If you think we have breached your privacy 15
5.1 Your right of internal review 15
5.1.1 Process 15
5.1.2 Timeframes 16
5.2 Your right to external review 16
5.3 Complaints to the Privacy Commissioner 16
6 Contact Us 17
7 Annexure A 18
Information Protection Principles 18
8 Annexure B 21
Health Privacy Principles 21

Author:	Senior Legal Counsel, Regulatory
Date:	July 2019
Version:	1
Reference:	Privacy Management Plan
Division:	Office of the Chief Executive - Legal
Review date:	June 2021

1 Introduction

1.1 Purpose

This Privacy Management Plan (plan) explains how Sydney Metro manages personal and health information under NSW privacy laws.

We have obligations under the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIPA**) and the *Health Records and Information Privacy Act 2002* (NSW) (**HRIPA**) to protect the privacy rights of customers, clients, staff and members of the public. We take these responsibilities seriously.

This plan also:

- illustrates our commitment to respecting the privacy rights of customers, clients, staff and members of the public, and enhances the transparency of our operations
- provides our employees and contractors with the necessary knowledge and skills to manage personal and health information appropriately
- meets the requirement for us to have such a plan under s 33 of PPIPA

1.2 Scope

This plan applies to our treatment of all personal and health information, whether it relates to a customer, an employee or another person (such as a contractor).

1.3 About Us

Sydney Metro is the NSW Government agency tasked with delivering the high-capacity, high-frequency Metro network across the Greater Sydney region. Our role is to plan, build, operate and optimise the door-to-door-to-door Metro customer journey. We are an operating agency within the Transport Cluster, contributing to an integrated public transport network serving a range of customers and communities. For further information about the Transport cluster, please see the Transport for NSW (TfNSW) website.

We are here to deliver for our State – maximising the social, economic and environmental opportunities and benefits catalysed by safe, reliable, turn-up-and-go services, and the delivery of vibrant, attractive precincts around our stations. In introducing new transport technology to Australia, we will be positioning ourselves at the forefront of commuter choice, and we recognise that effectively integrating transport and land use outcomes means being responsive to the needs of diverse communities along our alignments.

We collect, hold, use and disclose personal and health information for the purpose of carrying out these functions and activities.

Further information about Sydney Metro's functions and activities is available on our website.

1.4 The Information and Health Principles

Both PPIPA and HRIPA contain principles about managing personal and health information which we must comply with. These principles are legal obligations that describe what we must do when we collect, store, use or disclose personal and health information.

PPIPA sets out how we must manage personal information, and requires us to comply with 12 Information Protection Principles (IPPs).

HRIPA sets out how we must manage health information, and requires us to

comply with 15 Health Privacy Principles (HPPs).

A complete version of the IPPs and HPPs are included at Annexures A and B.

We explain how we manage personal and health information in Part 3.

1.5 What is personal information?

Personal information is defined in s 4 of PPIPA 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'.*

Essentially, personal information is any information or an opinion that is capable of identifying an individual.

Common examples of personal information include a person's name, bank account details, fingerprints, or a photograph or video.

1.5.1 What is not personal information?

There are certain types of information that are not considered personal information and these are outlined at ss 4(3) and 4A of PPIPA.

This means that the IPPs do not apply to our handling of certain types of information. These include:

- 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 (for example, information provided in a newspaper or a court judgment available on the internet)
- information or an opinion about an individual's suitability for appointment or employment as a public sector official (for example, recruitment records, referee reports and performance appraisals).

1.6 What is health information?

Health information is a specific type of personal information that is defined in s 6 of HRIPA as:

- personal information that is also information or an opinion about:
  - an individual's physical or mental health or disability
  - an individual's express wishes about the future provision of health services to themselves
  - a health service provided, or to be provided, to an individual
- other personal information collected to provide a health service
- other personal information about an individual collected in connection with the donation of an individual's body parts, organs or body substances
- genetic information that is or could be predictive of the health of a person or their relatives or descendants
- healthcare identifiers.

1.6.1 What is not health information?

As with personal information, there are certain types of information which are not considered health information. These are outlined in s 5(3) of HRIPA and include some of the types of information listed in Part 1.5.1.

For example, the results of a pre-employment medical check to assess a person's suitability for appointment or employment as a public official is not considered health information.

2 Personal and health information held by us

2.1 Types of personal and health information held by us

The collection of customer information is a central part of many of our functions and activities. We also have substantial obligations in respect of maintaining personal files and records of our staff.

As a consequence, we hold a large amount of personal and health information about customers and staff in a number of different locations and formats.

Some examples of the main types of personal and health information we (and TfNSW on our behalf) hold about our employees include:

- personal contact details and emergency contact details (including telephone number, postal and email address)
- date of birth
- financial information (such as salary, bank account information, tax file number)
- personnel information (such as attendance records, leave balances, educational and professional qualifications, training records)
- background information (such as criminal history, ethnic background, disability)
- health information (including medical certificates, reports and files, and fitness for duty assessments)
- statements and opinions
- audio recordings of telephone conversations and interviews
- photographs/footage
- injury management information such as workplace injuries, workers compensation claims and payments and return to work plans.

Some examples of the main types of personal and health information we hold about our customers and members of the public include:

- name and personal contact details (including telephone number, postal and email address)
- financial information (such as credit card information – for example, for the purpose of GIPA application fees)
- photographs/film/CCTV footage
- audio recordings (where incoming telephone conversations are recorded for quality and assurance purposes)
- opinions (general enquiries, consultation, feedback and complaints).

- We do not maintain any public registers for the purposes of PPIPA or HRIPA.

3 How we manage personal and health information

3.1 Introduction

This section provides an overview of how we comply with the IPPs and HPPs when we handle the personal and health information of our customers, clients, staff and members of the public.

In addition to our obligations under the IPPs and HPPs, our staff records are administered in accordance with the *NSW Government Public Service Commission Handbook*.

If you require further information about how privacy laws apply to a particular situation please contact the staff member or business area dealing with the information or contact us on the details in Part 6.

3.2 Collection

3.2.1 Collection for lawful purposes (IPP 1 & HPP 1)

We will only collect personal and health information if:

- it is for a lawful purpose that is directly related to one of our functions, and
- it is reasonably necessary for us to have the information.

We collect personal and health information in a variety of ways, including in writing, by email, through our website and social media, over the phone, by fax, recordings (such as CCTV footage) or in person.

We only ask for personal and health information that is reasonably necessary to the task at hand and is required for our functions and activities as outlined in Part 1.3.

We avoid collecting sensitive personal information if we don't need it. Sensitive information is information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

3.2.2 Direct collection (IPP 2 & HPP 3)

We generally collect personal or health information directly from the person concerned.

We will only collect information from a third party where:

- the person has authorised collection of the information from someone else
- the person is under 16 years of age – in which case we may instead collect personal information from the person's parent or guardian
- in the case of health information, it would be unreasonable or impracticable to collect information from an individual.

3.2.3 Requirements when collecting information (IPP 3 & HPP 4)

When collecting personal or health information from an individual, we take reasonable steps to tell them:

- the fact that the information is being collected
- what it will be used for
- what other parties (if any) routinely receive this type of information from us
- whether the collection is required by law (and if so, which law) or is voluntary
- what the consequences will be for the person if they do not provide the information to us
- that they have a right to access and/or correct their personal and health information held by us, and
- the name and contact details of the agency collecting and holding the information.

When collecting health information about an individual from a third party, we take reasonable steps to ensure the individual is generally aware of the notification matters above.

Generally, we provide this notification by way of a 'privacy notice' that is included on an application form, web page, recorded message or in a verbal notice at the time the personal or health information is collected, or as soon as we can afterwards.

Notification is not required if the information is not collected directly from the individual, except in the case of health information. In the case of health information, we are obliged to take reasonable steps to ensure the individual is generally aware of the notification matters except in certain circumstances (such as where collection from a third party is necessary or directly relevant and the individual to whom the information relates is unlikely to suffer burden or harm and is not discriminated against and decisions are not made about the individual).

3.2.4 Relevant (IPP 4 & HPP 2)

When collecting information from an individual, we will:

- not collect excessive personal or health information
- not collect personal or health information in an unreasonably intrusive manner, and
- ensure that personal and health information collected is relevant, accurate, up-to-date and complete

We take reasonable steps to ensure that information we collect from an individual is not unreasonably intrusive or excessive, and is relevant, accurate, up-to-date and complete.

To determine what might be reasonable steps, we consider:

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

3.3 Retention and security (IPP 5 & HPP 5)

We will take reasonable security safeguards to protect personal and health information from loss, unauthorised access, use, modification or disclosure, and against all other misuse. We will ensure personal and health information is stored securely, not kept longer than necessary, and disposed of appropriately.

Where it is necessary for personal or health information to be transferred to a person in connection with the provision of a service to us, we will take steps to prevent unauthorised use and disclosure of that information.

We hold a large amount of personal and health information and consider the security of that information fundamental to protecting privacy.

Information is stored in a variety of ways, including in our databases, cloud storage, by third parties and in various physical office locations.

We maintain reasonable security measures, including technical, physical and administrative actions, to protect information from unauthorised access and misuse.

Examples of such security measures include:

- restricting access to all IT systems and databases to ensure that only authorised users with a clear business need can access them
- use of strong passwords for computer access and a mandatory requirement that all staff change computer access passwords on a regular basis
- print on demand (secured printing)
- implementing and maintaining strong security software across all network components in arrangements for data transmission (including encryption and password protection where appropriate), backup and storage
- maintaining logs and audit trails which are monitored and retained on a regular basis
- providing staff with access to secure storage spaces near workstations to secure documents and devices
- physically securing sensitive and confidential information in locked rooms
- implementing and observing a clear desk policy
- maintaining and continually improving transport information security management systems that comply to ISO/IEC 27001:2013 standard
- align with our obligations under the NSW Cyber Security Policy 2019
- adopting best practice in electronic and paper records management and complying with our obligations under the *State Records Act 1998* (NSW)
- keeping information for only as long as necessary
- when no longer required, information is destroyed or disposed of in a secure manner where it is necessary for information to be transferred to a third party provider for the purposes of providing us with a service, we develop and execute contract terms that would prevent them from unauthorised use or disclosure of information that we hold
- providing mandatory information security awareness training to all Sydney Metro staff.

3.4 Accuracy and access

3.4.1 Transparency (IPP 6 & HPP 6)

We enable anyone to know:

- whether we are likely to hold their personal and health information
- the nature of the personal and health information
- the main purposes for which we use their personal and health information, and
- their entitlement to access their personal and health information.

We rely on the person providing the information to confirm its accuracy.

If you have any questions about the personal or health information held about you, please contact us on the details included at Part 6.

3.4.2 Access to personal and health information (IPP 7 & HPP 7)

We allow people to access their personal and health information without excessive delay or expense. We only refuse access where authorised by law, and we will provide written reasons, if requested.

Members of the public

Contact us on the details provided in Part 6.

Employees

Sydney Metro staff are able to access their personnel file by making a request to Transport Shared Services by contacting HR Advisory on 1800 618 445 or at tfnswhr@transport.nsw.gov.au.

Files about disciplinary matters and grievances are confidential and access is generally provided only to the staff member to whom the file relates. Generally staff may inspect files under supervision and will also be able to take photocopies of material on their file.

Access to information under GIPA

Anyone is able to seek access to government information that is held by us under the *Government Information (Public Access) Act 2009* (NSW) (**GIPA Act**). Sometimes the information that is requested includes personal and health information of other people. There are certain considerations that are taken into account before any information is released and we may withhold the personal or health information of another person. For more information about GIPA Act or making an access application, please visit the Transport for NSW website.

3.4.3 Alterations to personal and health information (IPP 8 & HPP 8)

We will allow people to update or amend their personal and health information, to ensure it is accurate, relevant, up-to-date, complete and not misleading. Where practicable, we will notify any other recipients of any changes.

We encourage you to help us keep any information we hold about you accurate, up-to-date and complete by contacting us with updated information.

If information we hold is accurate, relevant, up-to-date, complete and not misleading but a person still insists on an amendment, we can decline to do so, but must take reasonable steps to allow the person to add a statement about the requested changes to our records. For example, it may be appropriate to attach a statement, instead of amending the information, for a disputed medical diagnosis or a person with a criminal record maintaining their innocence.

Members of the public

Please contact us on the details provided in Part 6.

Employees

Employees are able to request amendment of their personal or health information by contacting HR Advisory on 1800 618 445 or at or at tfnswhr@transport.nsw.gov.au.

We encourage you to keep your personal information up to date and accurate, particularly information about your personal contact details and next of kin contact details so that you (or they) can be contacted in an emergency. It is also your responsibility to inform us if you wish to change your bank account details or payment details.

3.5 Use

3.5.1 Accuracy (IPP 9 & HPP 9)

Before using personal or health information, we will take reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.

We will take reasonable steps to ensure that personal and health information is still relevant and accurate before we use it.

3.5.2 Limited Use (IPP 10 & HPP 10)

We may use personal and health information for:

- the primary purpose for which it was collected
- a directly related secondary purpose
- another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health
- another purpose for which the person has consented, or
- another purpose where permitted by law.

When we use personal and health information, it means that we use it internally *within* Sydney Metro. This includes the provision of information to contractors engaged by Sydney Metro or TfNSW to manage information on our behalf in circumstances where Sydney Metro or TfNSW retains control over the handling and use of the information.

Generally, we only use personal and health information for the purpose for which is was collected. That purpose is set out in the privacy notice.

A directly related secondary purpose is a purpose that is very closely related to the purpose for collection and would be the type of purpose that people would quite reasonably expect their information to be used for.

Some examples of where the law permits us to use personal or health information for another (secondary) purpose include:

- quality assurance activities such as monitoring, evaluating and auditing
- work health and safety laws require that we use information to ensure the safety of our employees

- unsatisfactory professional conduct or breach of discipline
- the information relates to a person's suitability for appointment or employment as a public sector official
- finding a missing person
- preventing a serious threat to public health and safety.

3.6 Disclosure

3.6.1 Disclosure (IPPs 11 & 12 and HPPs 11 & 14)

We may disclose personal information if:

- the disclosure is directly related to the purpose for which the information was collected, and we have no reason to believe that the individual concerned would object to the disclosure
- the individual has been made aware in the privacy notice that information of the kind in question is usually disclosed to the recipient
- we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health, or
- where the disclosure is otherwise authorised by law.

Higher protections are afforded to sensitive personal information. We can generally only disclose sensitive personal information when the person has consented to the disclosure or when it is necessary to prevent a serious and imminent threat to life or health.

We can generally disclose health information when the person has consented to the disclosure; the disclosure is directly related to the purpose for which it was collected and the individual would reasonably expect us to disclose the information for that purpose; or the disclosure is necessary to prevent or lessen a serious and imminent threat to life, health or safety.

When we disclose information, it means that we give it to a third party outside of Sydney Metro to use the information for their own purposes. We will only do this in the circumstances outlined above, or when you have provided consent for us to do so or it is permitted or required to by law.

Generally, we do not disclose health information outside of NSW. However, if it is necessary to do so, we only disclose the information in accordance with PPIPA and HRIPA.

3.6.2 Identifiers (HPP 12)

We will only identify individuals by using unique identifiers if it is reasonably necessary for us to carry out our functions.

Identifiers are used to uniquely identify an individual and their health records. An identifier does not need to use a person's name as they are designed to be unique to a specific individual (for example, a customer number, unique patient number, tax file number, or driver licence number).

3.6.3 Anonymity (HPP 13)

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.

This HPP is not relevant to our functions and activities.

3.6.4 Linkage of Health Records (HPP 15)

We only use health records linkage systems if an individual has provided or expressed their consent, unless the linkage is for research purposes and has been approved in accordance with statutory guidelines.

We will only use health records linkage systems when individuals have expressly consented to their information being included on such a system, or for research purposes which have been approved by an Ethics Committee and in accordance with the Statutory Guidelines on Research.

3.7 Exemptions to how we manage personal and health information

3.7.1 Specific exemptions contained in PPIPA and HRIPA

PPIPA and HRIPA provide that we need not comply with some or all of the IPPS and HPPs if certain circumstances apply.

Some examples of exemptions most relevant to our functions and activities include:

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- use or disclosure for law enforcement purposes or investigative functions
- where another law authorises or requires us not to comply
- where non-compliance is lawfully authorised or required
- where compliance would prejudice the individual
- when we exchange information with other public sector agencies
- some research purposes.

If an exemption applies to a particular situation, we will inform the individual(s) concerned about the exemption and why it applies.

3.8 Offences

Both PPIPA and HRIPA contain criminal offence provisions applicable to public sector officials and persons who misuse personal and health information.

Our staff are regularly reminded of their responsibilities under PPIPA and HRIPA and these obligations are reinforced in our Code of Conduct and through initiatives outlined in Part 4.

4 Strategies for compliance and best practice

4.1 Introduction

We are committed to protecting the privacy rights of customers, clients, staff and members of the public.

We adopt several strategies to implement best practice principles and comply with our obligations under PPIPA and HRIPA that recognise that privacy is a shared responsibility within the agency.

4.2 Policies and procedures

We have adopted a number of policies, standards and guidelines to inform and assist staff in protecting privacy. These policies provide best

practice guidance and practical advice on matters relating to:

- acceptable use of technology
- dealing with confidential information
- information security
- records management
- privacy breaches
- use of social media.

Our Code of Conduct outlines the responsibilities of our staff in protecting privacy in the course of their duties. All staff are provided with a copy of the Code and are regularly reminded of their obligations. The Code is available on our intranet and the Transport for NSW website.

We consistently review and update our policies and procedures when necessary.

Policies and procedures, including this plan, are communicated to staff in a range of ways, including through our intranet, printed copies and targeted and on-the-job training.

4.3 Promoting privacy awareness

We undertake a range of initiatives to ensure our staff and members of the public are informed of our privacy practices and obligations under PPIPA and HRIPA. This also assists in identifying and mitigating risks associated with privacy and encourages best practice.

We promote privacy awareness and compliance by:

- publishing and promoting this plan on our intranet and website
- including mandatory privacy training in our induction program (for example, Code of Conduct and Fraud and Corruption awareness modules)
- publishing and promoting all policies on our intranet
- maintaining a dedicated privacy page on our intranet that centralises all privacy resources for staff and provides information about what to do if staff are unsure about a privacy issue
- participating annually in Privacy Awareness Week
- delivering periodic face to face training across different business areas
- assessing privacy impacts of new projects or processes from the outset
- endorsing a culture of good privacy practice
- educating the public about their privacy rights and our obligations (for example, providing privacy information on forms that collect personal and health information).

4.4 Review and continuous improvement

We are committed to identifying opportunities for improvement and better practice in protecting the privacy of our customers, staff and members of the public.

We consistently evaluate the effectiveness and appropriateness of our privacy practices, policies and procedures to ensure they remain effective and identify, evaluate and mitigate risks of potential non-compliance.

We are committed to:

- monitoring and reviewing our privacy processes regularly
- further promoting and maintaining privacy awareness and compliance
- encouraging feedback from our staff and customers on our privacy practices
- actively participating in Privacy Awareness Week and other privacy initiatives

- introducing initiatives that promote good privacy handling in our business practices (such as assessing privacy impacts of new projects or processes from the outset)
- maintaining and continually expanding the scope of Transport information security management systems that align to ISO/IEC 27001:2013 standard
- carrying out comprehensive assessments of the risk to digital information and digital information systems that are used to process personal and health information
- actively promote information security awareness to ensure all staff fully understand their responsibilities of information security compliance in their day-to-day activities

Sydney Metro participates in a Transport wide Privacy Forum comprising of representatives from all Transport agencies. The Forum meets regularly to discuss privacy issues and identify opportunities for better practice in protecting privacy.

5 If you think we have breached your privacy

We encourage you to contact us directly to resolve any concerns you have about our handling of your personal or health information.

If you think we have breached your privacy, we encourage you to discuss any concerns with the staff member or business unit dealing with your information, or contact us on the details provided in Part 6.

5.1 Your right of internal review

You have the right to ask us for an internal review if you think we have breached your privacy.

An application for internal review must:

- be in writing
- be addressed to Sydney Metro
- specify an address in Australia to which you can be notified after the completion of the review.

To apply for an internal review, you can send your application and any relevant material by email or post to us at the details provided in Part 6.

5.1.1 Process

The internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint
- is a staff member of Sydney Metro, and
- is qualified to deal with the subject matter of the complaint.

Internal review follows the process set out in the Information & Privacy Commission's *internal review checklist*. When the internal review is completed, the applicant will be notified in writing of:

- the findings of the review
- the reasons for those findings
- the action we propose to take
- the reasons for the proposed action (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal.

We are required to give a copy of your internal review request to the Privacy Commissioner. We will also send a copy of the draft internal review report to the Privacy Commissioner and we must take into account any submissions made by the Privacy Commissioner. We will keep the Privacy Commissioner informed of the progress of the internal review and will provide a copy of the finalised internal review report.

5.1.2 Timeframes

You must lodge your request for internal review within six months from the time you first became aware of the conduct that you think breached your privacy.

We may accept late applications in certain circumstances (such as if you have only become aware of your right to seek an internal review or for reasons relating to your capacity to lodge an application on time). If we do not accept your application, we will provide our reasons in writing.

We will acknowledge receipt of an internal review and will aim to:

- complete the internal review within 60 calendar days, and
- respond to you in writing within 14 calendar days of completing the internal review.

We will contact you to advise how long the review is likely to take, particularly if it may take longer than expected.

If the internal review is not completed within 60 days, you have a right to seek a review of the conduct by the NSW Civil and Administrative Tribunal (see below).

5.2 Your right to external review

You have the right to apply to the NSW Civil and Administrative Tribunal if you have sought an internal review and:

- you are not satisfied with the outcome of the internal review
- you are not satisfied with the action taken in relation to your application for internal review
- you do not receive an outcome of the internal review within 60 days.

For more information about seeking an external review, contact the Tribunal on the details below:

Office: NSW Civil and Administrative Tribunal (NCAT)
Administrative and Equal Opportunity Division
Level 10, John Maddison Tower
86-90 Goulburn Street
Sydney NSW 2000

Phone: 1300 006 228

Website: www.ncat.nsw.gov.au

5.3 Complaints to the Privacy Commissioner

You have the option of complaining directly to the Privacy Commissioner if you believe that we have breached your privacy.

The Privacy Commissioner's contact details are:

Office: Information & Privacy Commission
Level 3, 47 Bridge Street
Sydney NSW 2000

Post: PO Box R232
Royal Exchange NSW 2001

Phone: 1800 472 679

Fax: 02 8114 3756

Email: ipcinfo@ipc.nsw.gov.au

6 Contact Us

For further information about this plan or questions about your privacy, please contact us on the details below.

Web: www.sydneymetro.info

Post: Information & Privacy Unit
Transport for NSW
PO Box K659
Haymarket NSW 1240

Phone: 02 8202 3862

Email: privacy@transport.nsw.gov.au

7 Annexure A

Information Protection Principles

IPP	Full text from the *Privacy and Personal Information Protection Act 1998* (Part 2, sections 8-19)
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.
2	**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.
3	**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, (f) the name and address of the agency that is collecting the information and the agency that is to hold the information.
4	**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.
5	**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.

IPP	Full text from the *Privacy and Personal Information Protection Act 1998* (Part 2, sections 8-19)
6	**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.
7	**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.
8	**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. (6) 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.
9	**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.
10	**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.

IPP	Full text from the *Privacy and Personal Information Protection Act 1998* (Part 2, sections 8-19)
11	**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.
12	**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 about an individual 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) the public sector agency 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 information protection principles, or (b) the individual expressly consents to the disclosure, or (c) the disclosure is necessary for the performance of a contract between the individual and the public sector agency, or for the implementation of pre-contractual measures taken in response to the individual's request, or (d) the disclosure is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the public sector agency and a third party, or (e) all of the following apply: (i) the disclosure is for the benefit of the individual, (ii) it is impracticable to obtain the consent of the individual to that disclosure, (iii) if it were practicable to obtain such consent, the individual would be likely to give it, or (f) the disclosure is reasonably believed by the public sector agency to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or (g) the public sector agency has taken reasonable steps to ensure that the information that it has disclosed will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles, or (h) the disclosure is permitted or required by an Act (including an Act of the Commonwealth) or any other law. (3)–(5) (Repealed)

8 Annexure B

Health Privacy Principles

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
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	**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	**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	**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

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
	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	**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. **Note.** 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	**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	**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. **Note.** 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

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
	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	**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. **Note.** 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	**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	**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) **Consent** the individual to whom the information relates has consented to the use of the information for that secondary purpose, or (b) **Direct relation** the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose, or **Note.** For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose. (c) **Serious threat to health or welfare** 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) **Genetic information**

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
	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) **Management of health services** 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) **Training** 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) **Research** 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) **Find missing person** 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) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline** the organisation: (i) has reasonable grounds to suspect that: (A) unlawful activity has been or may be engaged in, or

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
	(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) **Law enforcement** 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) **Investigative agencies** 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) **Prescribed circumstances** 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	**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) **Consent** the individual to whom the information relates has consented to the disclosure of the information for that secondary purpose, or (b) **Direct relation** the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or **Note.** For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose. (c) **Serious threat to health or welfare** 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

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
	(ii) a serious threat to public health or public safety, or (c1) **Genetic information** 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) **Management of health services** 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) **Training** 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) **Research** 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) **Compassionate reasons** 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,

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
	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) **Find missing person** 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) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline** 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) **Law enforcement** 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) **Investigative agencies** 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) **Prescribed circumstances** 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

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
	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	**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	**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	**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

HPP	Full text from the *Health Records and Information Privacy Act 2002* (Schedule 1)
	(h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.
15	**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.