Sydney Opera House

Privacy Management Policy and Plan

October 2016

Contents

1 Overview

1.1 Policy statement

The Sydney Opera House is operated and maintained for the Government of New South Wales by the Sydney Opera House Trust (the **Opera House**), which is constituted as a body corporate under the *Sydney Opera House Trust Act 1961*.

The Opera House's objectives and functions are to: administer, care for, control, manage and maintain the Sydney Opera House building and site; manage and administer the site as an arts centre and meeting place; promote artistic taste and achievement in all branches of the performing arts; foster scientific research into and encourage the development of new forms of entertainment and presentations.

In connection with the carrying out of its functions, the Opera House collects personal and health information. The Opera House is committed to protecting the privacy of individuals by ensuring that the collection, storage, use and disclosure of personal and health information is undertaken in accordance with the requirements of the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) and the *Health Records and Information Privacy Act 2002* (**HRIP Act**) and with reference to this Plan. The Opera House complies with its obligations under these Acts in relation to personal and health information that is collected about its employees (including contractors), partners, performers, customers and members of the general public as set out in section 3 of this Plan.

1.2 Purpose

The purpose of this Privacy Management Plan is to:

- provide staff with the knowledge to manage personal and health information in accordance with the law;
- demonstrate to members of the public how the Opera House meets its obligations under the PPIP Act and the HRIP Act; and
- meet the requirement for the Opera House to have such a Plan under section 33 of the PPIP Act.

1.3 Responsibilities

Managers and Supervisors

Managers and supervisors are responsible for ensuring that their staff are aware of their privacy responsibilities under the PPIP and HRIP Acts and comply with this Plan.

Staff

All employees and contractors of the Opera House are required to comply with the PPIP and HRIP Acts and this Plan.

It is an offence for any person employed or engaged by the Opera House (including former employees or contractors) to intentionally use or disclose any personal information about another person, to which the employee or contractor has or had access in the exercise of his or her official functions (other than in connection with the lawful exercise of his or her functions).

Privacy Officer for the Opera House

The Opera House has appointed a Privacy Officer who handles all matters related to privacy, including the handling of personal and health information.

The role of the Privacy Officer is to:

- ensure this Plan remains up to date (including monitoring and continuously improving this Plan);
- make a copy of this Plan available to all current and new employees and contractors;
- train and educate staff (with the assistance of members of the Learning and Development team) in aspects of the PPIP and HRIP Acts;
- provide advice to staff and the Executive on privacy and the application of the PPIP and HRIP Acts;
- provide a first point of contact for members of the public for all matters related to privacy and the handling of personal and health information within the Opera House;

- participate in the development of new initiatives within the Opera House that have a potential privacy impact;
- conduct internal reviews into possible breaches of the PPIP and HRIP Acts; and
- liaise with the NSW Information and Privacy Commission and other government agencies.

The Privacy Officer can be contacted on the details below:

Post: Privacy Officer
Sydney Opera House
Bennelong Point
SYDNEY NSW 2000

Phone: 02 9250 7872

Email: privacy@sydneyoperahouse.com

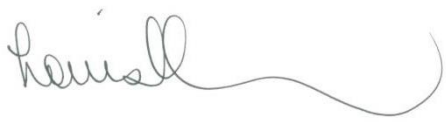
1.4 Review

The Plan will be reviewed and updated every 3 years at a minimum, or from time to time in response to legislative amendments and improvements in technology.

1.5 Approval

This Privacy Management Plan has been approved by the Chief Executive Officer of the Opera House.

APPROVED



Chief Executive Officer

Date: 19 October 2016

2 Personal and health information held by the Opera House

2.1 What is personal information?

Personal information is information or an opinion about an individual whose identity is apparent or could reasonably be ascertained from the information or opinion. Common examples of personal information include:

- a person's name;
- bank account details;
- fingerprints; or
- a photograph or video.

It can also include information or an opinion that is recorded (for example on paper or contained in a database) and also information or an opinion that is not recorded (for example verbal conversations). A person's identity may be apparent where neither their name nor a photograph is involved, but the information about the person is such that it could not be referring to anyone else.

There are 13 exclusions to the definition of personal information under the PPIP Act, including:

- 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; and
- information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Common examples of information falling within the exclusions include the recruitment records, referee reports and performance appraisals of prospective, current, and past Sydney Opera House employees, as well as information provided in the White Pages, a newspaper or a court judgment available on the internet.

For more information on these exclusions refer to sections 4(3) and 4A of the PPIP Act or contact the Privacy Officer.

2.2 What is health information?

Health information means:

- personal information that is also information or an opinion about:
  - a person's physical or mental health or disability;
  - a health service provided, or to be provided, to a person;
  - a person's express wishes about the future provision of health services to themselves;
- other personal information collected to provide, or in providing, a health service;
- 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
- other personal information that is genetic information arising from a health service provided to a person in a form that is or could be predictive of the health of that person or a genetic relative of that person.

There are 15 exclusions to the definition of health information under the HRIP Act, which include the exclusions listed above at section 2.1of this Plan. An example of information excluded by the HRIP Act is the results of a pre-employment medical check to assess a person's suitability for a job as a public sector official.

For more information on these exclusions, refer to section 5(3) of the HRIP Act or contact the Privacy Officer.

2.3 Main kinds of personal and health information held by the Opera House

The Opera House holds a range of personal and health information in a number of locations and in a range of formats. Some examples of the main kinds of personal and health information held by the Opera House about our employees (and contractors) include:

- personal information contained in or related to personnel records, including emergency contact details, date of birth, financial information (including bank account information and tax file numbers), educational qualifications, ethnic background, timesheets, grade and salary range;
- health information contained in or related to personnel records, including medical certificates, fitness for duty assessments, injury management information (such as workplace injuries incident reports, workers compensation claims and payments and return to work plans);
- personal and health information, including complainant details, audio recordings, images and CCTV footage held for the purposes of conducting workplace investigations (which must be conducted in accordance with the *Workplace Surveillance Act 2005*); or
- personal and health information related to audit and risk work, including audit evidence collected during the performance of approved audit programs, fraud and corrupt conduct complaints and conflict of interest disclosures.

Some examples of the main kinds of personal and health information held by the Opera House about our partners, performers, customers and members of the general public include:

- personal and health information related to the purchase of tickets that is collected so that we can deliver tickets to customers, contact customers in the event of performance postponement or cancellation, or when other important information must be provided to customers including, but not limited to, difficulties relating to purchases. This information could include name and personal contact details (including telephone number, postal and email address), financial information (including credit card information), date of birth and Roads and Maritime permit and concession numbers;
- personal information that may be collected when customers join *Sydney Opera House Insiders*, subscribe to our mailing lists, enter competitions, participate in promotional activities, provide feedback or make a donation to the Opera House through any channel;
- photographs and CCTV footage recorded while customers are within the Opera House precinct;
- opinions arising from general enquiries, consultation, feedback and complaints; or
- health information as a result of having provided First Aid on the Opera House premises.

3 How the Opera House manages personal and health information

3.1 Introduction

The objectives of the PPIP and HRIP Acts are to protect individuals' privacy, to allow them a degree of control over information held about them by public sector agencies and to provide a mechanism for complaints. These objectives are achieved primarily through compliance with 'privacy principles', which establish standards for using personal information in the NSW public sector and regulate the collection, storage, use and disclosure of personal and health information by agencies.

For the purposes of this Plan, the most relevant obligations and how the Opera House complies with these obligations have been condensed into one set of plain language principles below. These principles should not be treated as a substitute for the principles set out in the PPIP and HRIP Acts as they do not cover the full range or complexity of the principles. Staff should always seek guidance from the Privacy Officer in relation to the application of these principles.

3.2 Condensed Information Protection Principles and Health Privacy Principles

The references in brackets are to the Information Protection Principles (**IPP**) in the PPIP Act and the Health Privacy Principles (**HPP**) in the HRIP Act.

COLLECTION	
Limiting the collection of personal and health	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.

information *(s. 8 PPIP Act and HPP 1*)	By limiting our collection of personal and health information to only what we reasonably need, it is much easier to comply with our other privacy obligations. When requesting personal or health information on behalf of the Opera House, staff should only ask for information that is reasonably necessary to the task at hand. We will especially avoid collecting sensitive personal information if we do not need it. See the Definitions in Section 9 of this Plan for an explanation of what constitutes sensitive personal information.
Collecting personal and health information – the source, method and content *(ss. 9 & 11 PPIP Act and HPP 2 & 3)*	We will collect personal or health information directly from the person unless they have authorised otherwise or, in the case of health information, it would be unreasonable or impractical to obtain the information directly from the individual. When collecting information from an individual, we will: ▪ not collect excessive personal or health information; ▪ not collect personal or health information that would unreasonably intrude in that individual's personal affairs; and ▪ ensure that personal and health information collected is relevant, accurate, up-to-date and complete.
Notification on collection *(s. 10 PPIP Act and HPP 4)*	When collecting personal or health information from an individual (or from someone else about that individual), we will take reasonable steps to tell the person: ▪ that the Opera House is collecting and holding the information, and provide our contact details; ▪ 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; and ▪ that they have a right to access and/or correct their personal and health information held by us. Notification is usually provided to individuals through a 'privacy notice' at the initial time of collection or as soon as we can afterwards. Privacy notices can be in writing or verbal. A copy of our Customer Privacy Statement, which serves as our notice, is available on our website at this link. This document is also publicly available on our website.
STORAGE	
Retention and security *(s. 12 PPIP Act and HPP 5)*	We will put in place 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 for lawful purposes and disposed of appropriately. Where it is necessary for personal or health information to be transferred to a third party in connection with the provision of a service to us, we will do everything reasonably within our power to prevent unauthorised use and disclosure of that information. Information security is fundamental to information privacy. Our information technology systems are designed to ensure that only authorised users can access them. Access controls are also employed to only give access to information required for the user's particular role and functions. Logs and audit trails will act as

	a deterrent against any misuse, and enable security breaches or data quality problems to be investigated. We follow best practice in records management for both electronic and paper records and apply retention periods and disposal schedules in accordance with the *State Records Act 1998*. When no longer required, we destroy personal and health information in a secure manner as appropriate.
Transparency *(s. 13 PPIP Act and HPP 6)*	We will enable anyone to know, on request to the Opera House Privacy Officer: ▪ whether we hold their personal or health information; ▪ the nature of the personal or health information; ▪ the main purposes for which we use their personal or health information; and ▪ their entitlement to access their personal or health information. The publication of this Plan promotes accountability and increases the transparency of our information handling practices. This Plan will be accessible on our website and available to download and print. For more information on our privacy practices, staff and members of the public can contact the Opera House Privacy Officer.
Access and alteration *(ss. 14 & 15 PPIP Act and HPP 7 & 8)*	We will allow people to access their personal and health information without excessive delay or expense. We will allow, and encourage, people to update or amend their personal and health information, to ensure it is accurate, relevant, up-to-date, complete and not misleading. We will only refuse access or a request to amend personal or health information where authorised by law, and we will provide written reasons, if requested. Further information about how to access and amend personal and health information held by the Opera House is provided in section 4.1.
USE	
Accuracy *(s. 16 PPIP Act and 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 ensure that information is recorded in a consistent format and attempt to confirm the accuracy of information collected from a third party or a public source where practicable. We will not use personal or health information that we know is based on misleading or erroneous information.
Purpose of use *(s. 17 PPIP Act and HPP 10)*	We may use personal and health information for: ▪ the primary purpose for which it was collected; ▪ a directly related secondary purpose (where in the case of health information, the individual would reasonably expect us to use the information for that purpose); ▪ another purpose permitted by law, such as where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health; or ▪ another purpose for which the person has consented.
DISCLOSURE	
Disclosure *(ss. 18 & 19*	We may disclose personal information if: ▪ the disclosure is directly related to the purpose for which the information was

PPIP Act and HPPs 11 & 14)	collected, and we have no reason to believe that the individual concerned would object to the disclosure, ▪ the individual has been made aware in accordance with a privacy notice under section 10 of the PPIP Act that information of the kind in question is usually disclosed to the intended recipient, or ▪ we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health. Higher protections are afforded to certain sensitive personal information, as defined in Section 9 of this Plan. 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 may disclose health information if: ▪ 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 permitted by law, such as where it is reasonably necessary to prevent or lessen a serious and imminent threat to life, health or safety. We will not transfer personal or health information outside of NSW or to a Commonwealth agency except in limited circumstances permitted by law.

3.3 Exemptions from compliance with IPPs and HPPs

The PPIP Act and HRIP Act provide that we do not need to comply with some or all of the IPPs or HPPs if certain circumstances apply. Some examples of exemptions most relevant to our functions and operations include:

- where the receipt of health information is unsolicited;
- where another law authorises or requires us not to comply with the principles;
- where another law permits non-compliance with certain principles.
- where disclosure of information is reasonably necessary for the protection of public revenue, or in order to investigate an offence where there are reasonable grounds to believe that an offence may have been committed; and
- when we exchange personal information with other public sector agencies for certain purposes such as responding to correspondence from a Minister or the Premier.

4 How to access and amend personal and health information

4.1 Request to access and amend

You may request access to and/or alteration of your personal or health information by email or post. All requests should be sent to:

Post: Privacy Officer
Sydney Opera House
Bennelong Point
SYDNEY NSW 2000
Email: privacy@sydneyoperahouse.com

Your request should:

- include your name and contact details (postal address, telephone number and email address if applicable);
- state whether you are making the application under the PPIP Act (personal information) or the HRIP Act (health information);
- explain what personal or health information you want to access or amend; and
- explain how you want to access or amend it.

If staff want to access and/or amend their personnel file, a request may be made to Human Resources. Staff may inspect their files under supervision after obtaining approval from their Director.

5 Privacy complaints and internal reviews

A person who wishes to make a complaint in relation to privacy may do any of the following:

- make an informal complaint by contacting the Opera House Privacy Officer;
- make a complaint with the Privacy Commissioner; or
- make a formal complaint with the Opera House by applying for an internal review.

5.1 How to make an informal complaint

We encourage people to try to resolve privacy concerns with us informally by simply contacting the Opera House Privacy Officer to discuss the issue, before lodging an application for internal review.

5.2 How to make a complaint with the Privacy Commissioner

You may make a privacy complaint directly to the Privacy Commissioner if you believe that the Opera House has breached an Information Protection Principle (**IPP**) in the PPIP Act or a Health Privacy Principle (**HPP**) in the HRIP Act.

For more information on how the Privacy Commissioner handles privacy complaints received from members of the public, please refer to the Information & Privacy Commission's *Protocol for Handling Privacy Complaints*. Complaints directed to the Privacy Commissioner can only result in conciliated outcomes, whereas internal reviews (which are explained below) can lead to a binding determination by the NSW Civil and Administrative Tribunal (the **Tribunal**).

The Privacy Commissioner can be contacted as follows:

Office: Information & Privacy Commission Level 11, 1 Castlereagh Street Sydney NSW 2000
Post: GPO Box 7011 Sydney NSW 2001
Phone: 1800 472 679
Fax: 02 8114 3756
Email: ipcinfo@ipc.nsw.gov.au

5.3 How to apply for an internal review by the Opera House

A person who is aggrieved by the conduct of the Opera House in relation to personal or health information is entitled to an internal review of that conduct by the Opera House. An internal review is the process by which we manage formal, written privacy complaints.

An application for internal review must:

- be in writing;
- be addressed to the Opera House and sent by email or post;
- specify an address in Australia to which the applicant is to be notified after the completion of the review; and
- be lodged with the Opera House within **six months** from the time the applicant first became aware of the conduct that they want reviewed.

The Opera House may, on a case by case basis, accept applications for internal review where the six month time limit has been exceeded. Reasons for lateness should be clearly set out in the written application.

An application for internal review can be made on behalf of someone else. Where the applicant is not literate in English (for example, because it is not their first language), and where there is no other organisation making the application on their behalf, staff should help the person to write their application. Staff should use a professional interpreter, if necessary. Applications in languages other than English will be accepted and translated, and all acknowledgments and correspondence to the applicant will be translated.

Applications for internal review or any written complaint about privacy received by staff should be forwarded to the Opera House Privacy Officer.

5.4 Internal review process

When we receive an internal review application the Opera House Privacy Officer will:

- send an acknowledgment letter to the applicant within five working days and advise that if the internal review is not completed within **60 days** they have a right to seek a review of the conduct by the Tribunal; and
- as soon as practicable, send a letter to the Privacy Commissioner with details of the application. The Opera House will keep the Privacy Commissioner informed of the progress of the internal review.

Internal review follows the process set out in the Information & Privacy Commission's *Internal Review Checklist* which is attached at **Appendix A**.

If the complaint is about an alleged breach of the IPPs, HPPs, privacy code of practice or health privacy code of practice, the internal review will be conducted by the Opera House Privacy Officer or by another person who:

- was not involved in the conduct which is the subject of the complaint;
- is an employee or an officer of the Opera House; and
- is qualified to deal with the subject matter of the complaint.

When the internal review is completed, as soon as reasonably practicable and within **14 calendar days** the Opera House Privacy Officer will notify the applicant in writing of:

- the findings of the review;
- the reasons for those findings;
- the action the Opera House proposes to take;
- the reasons for the proposed action (or no action); and
- the applicant's entitlement to have the findings and the proposed action reviewed by the Tribunal.

We will also send a copy of that letter to the Privacy Commissioner.

5.5 External review by the NSW Civil and Administrative Tribunal

Individuals can seek an external review if they are not satisfied with the outcome of an internal review we have conducted or with the Opera House's action in relation to the individual's application for internal review. Individuals can also seek an external review if they do not receive an outcome of the review within **60 days**.

To seek an external review, a person must apply to the Tribunal. Generally a person must seek an internal review before they have a right to seek an external review.

The Tribunal has the power to make binding decisions, and may make orders requiring us to (among other things):

- refrain from any conduct or action which breaches an IPP, HPP, privacy code of practice or health privacy code of practice;
- perform in compliance with an IPP, HPP, privacy code of practice or health privacy code of practice;
- correct information disclosed by the Opera House; or
- take steps to remedy loss or damage.

The Tribunal may also make an order requiring us to pay damages of up to $40,000 if the applicant has suffered financial loss, or psychological or physical harm because of the conduct of the Opera House.

For more information about seeking an external review including current forms and fees, please contact the Tribunal:

Office: NSW Civil and Administrative Tribunal (NCAT)
Level 10, John Maddison Tower 86-90 Goulburn Street
SYDNEY NSW 2000
Phone: 1300 006 228 or 02 9377 5859 (TTY)
Website: www.ncat.nsw.gov.au

6 Strategies for implementing this Plan

Policies and procedures, including this Plan, are communicated to staff in a range of ways, including through the Opera House intranet, printed copies and training. All new staff are required to complete an online module on the Code of Conduct and an induction course before starting with the Opera House. The Code of Conduct specifically refers to the importance of protecting privacy and complying with the PPIP Act and the HRIP Act.

All policies and procedures are sourced, numbered, dated and owned by a specific management position, and are systematically reviewed and updated when necessary.

Any new policy or procedure, or any policy that is changed or updated, is developed and reviewed in consultation with relevant business areas and receives the endorsement of senior management, including the General Counsel and Chief Executive Officer.

The Opera House advises members of the public about its privacy obligations and the public's privacy rights through the publication of this Plan on the Opera House website and by providing/making available the Opera House's *Customer Privacy Statement*.

7 Privacy and other legislation relating to personal and health information

7.1 Links to relevant Privacy legislation

- *Privacy and Personal Information Protection Act 1998;*
- *Health Records and Information Privacy Act 2002*;
- *Privacy and Personal Information Protection Regulation 2014*;
- *Health Records and Information Privacy Regulation 2012*.

7.2 Other legislation

Other legislation that may also affect the application of the privacy principles to the Opera House includes, but is not limited to, the following:

- *Government Information (Public Access) Act 2009*;
- *State Records Act 1998;*
- *Workplace Surveillance Act 2005*;
- *Surveillance Devices Act 2007*;
- *Ombudsman Act 1974*; and
- *Public Interest Disclosures Act 1994*.

Copies of this legislation can be found on the NSW Legislation website.

8 Related Opera House policies

Closed Circuit Television Policy

Code of Conduct

Information Systems and Security Policy

Records Management Policy

9 Definitions

Collection refers to the way in which the Opera House acquires or gathers personal or health information. Collection can be by any means, including a written or online form, a verbal conversation, a voice recording or taking a picture or image.

Disclosure means when the Opera House makes known to an individual or body, personal or health information that the individual or body did not previously know.

Health information is a subset of personal information. Health information relates to the physical or mental health or disability of an individual or information provided or generated in the delivery of a health service. See section 6 of the HRIP Act for the full definition.

Holding personal and health information: information is held by the Opera House if it is in possession or control of the information, including when the information is in the possession or control of a person employed or engaged by the Opera House in the course of such employment or engagement. This means that the Opera House will be considered to hold personal or health information if it is processed by a contractor or service provider on behalf of the Opera House and will remain responsible for how the Opera House contractors or service providers handle such information in accordance with the privacy principles.

Information & Privacy Commission is an independent NSW Government agency with responsibilities to promote privacy rights for the people of NSW. The Commission is headed by the Information Commissioner and the Privacy Commissioner. See www.ipc.nsw.gov.au for more details.

Personal information is information or an opinion that identifies or could reasonably identify an individual. See section 4 of the PPIP Act for the full definition.

Privacy principles refer to the Information Protection Principles set out in Division 1 of Part 2 of the PPIP Act and the Health Privacy Principles set out in Schedule 1 of the HRIP Act. The privacy principles set out the baseline standards for all NSW public sector agencies when handling personal or health information.

Public sector official is generally a person who is employed by or acts for or on behalf of a public sector agency, or employed in the Government Service. See section 3(1) of the PPIP Act and section 4(1) of the HRIP Act for the full definition.

Sensitive personal information refers to personal information about an individual's race, ethnicity, religion, sexual activities, political or philosophical beliefs or membership of a trade union.

Staff means all permanent and temporary staff, staff seconded from another organisation, contractors and consultants.

Unsolicited information refers to personal or health information that the Opera House finds itself receiving without having asked for it.

Appendix A – IPC's Internal Review Checklist

information and privacy commission new south wales

Privacy Internal Review Checklist

July 2014

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

A privacy complaint may come under:

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

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

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

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

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

Preliminary steps

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

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

☐ No – follow your agency's normal complaint handling procedures.

Note: "Personal information" is defined at s.4 of the PPIP Act as "information or an opinion… about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion". There are some exemptions to the definition (e.g. for "information or an opinion about an individual's suitability for appointment or employment as a public sector official") so check s.4 in full. However if you are thinking of relying on one of these exemptions, especially s.4(3)(b) or s.4(3)(j), please first seek advice from the Information and Privacy Commission NSW (IPC) as to the extent to which the exemption applies.

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

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

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

☐ Both – See the notes below.

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

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

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

_____

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

☐ Yes – go to Q.5.

☐ No – the PPIP Act does not apply. Follow your agency's normal complaint handling procedures.

5. Is the complaint about health information and conduct that occurred after 1 September 2004?

☐ Yes – the HRIP Act covers this complaint.

☐ No – the PPIP Act covers this complaint.

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

_____

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

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

_____

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

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

Will you accept this late application?

☐ Yes – go to Q.9.

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

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

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

_____

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

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

- ☐ Collection of the complainant's personal information (IPPs 1-4)
- ☐ Security or storage of the complainant's personal information (IPP 5)
- ☐ Refusal to let the complainant access or find out about their own personal information (IPPs 6-7)
- ☐ Accuracy or relevance of the complainant's personal information (IPPs 8-9)
- ☐ Use of the complainant's personal information (IPP 10)
- ☐ Disclosure of the complainant's personal information (IPPs 11-12, and/or the public register provisions in Part 6 of the Act)
- ☐ Other / it's not clear

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

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

- ☐ Collection of the complainant's health information (HPPs 1-4)
- ☐ Security or storage of the complainant's health information (HPP 5)
- ☐ Refusal to let the complainant access or find out about their own health information (HPPs 6-7)
- ☐ Accuracy or relevance of the complainant's health information (HPPs 8-9)
- ☐ Use of the complainant's health information (HPP 10)
- ☐ Disclosure of the complainant's health information (HPP 11)
- ☐ Assignment of identifiers to the complainant (HPP 12)
- ☐ Refusal to let the complainant remain anonymous when entering into a transaction with your agency (HPP 13)
- ☐ Transfer of the complainant's health information outside New South Wales (HPP 14)
- ☐ Including the complainant's health information in a health records linkage system (HPP 15)
- ☐ Other / it's not clear

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

12. Insert the reviewing officer's name here:

_____

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

13. Write to the complainant, stating:

- your understanding of the conduct complained about;
- your understanding of the privacy principle/s at issue (either IPPs at Q.10 or HPPs at Q.11);
- that the agency is conducting an Internal Review under the PPIP Act or the HRIP Act, as appropriate;
- the name, title, and contact details of the reviewing officer;

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

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

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

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

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

14. Send notice of the application (s54 PPIP) at Q.13 to:

NSW Privacy Commissioner
GPO Box 7011, SYDNEY NSW 2001

Or fax (02) 8114 3756

or email ipcinfo@ipc.nsw.gov.au

Include a copy of the complainant's application – either the written request or the information provided on the Privacy Complaint: Internal Review Application Form.

You can now start the review itself

15. a) Under the PPIP Act, you need to determine:

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

b) Under the HRIP Act, you need to determine:

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

16. It is recommnended that four weeks after sending the notice that an application has been received at Q.13, you send a progress report to the Privacy Commissioner and (If required) the complainant, including:

- details of the progress of the review;
- if there are delays, you may wish to provide an explanation of this and a revised estimated completion date for the review process; and
- a reminder that if the review is not complete by the date at Q.9, the complainant can go to the Tribunal for an external review of the alleged conduct and the relevant timeframe to apply for a Tribunal review.

On completion of the review

17. a) Under the PPIP Act, you need to determine:

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

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

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

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

b) Under the HRIP Act, you need to determine:

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

Notes: Don't forget to look at all the HPPs, as they can be inter-related. For example a complaint about disclosure (HPP 11) might also raise issues about data security under HPP 5, or notification about collection at HPP 4.

Exemptions are found in the HRIP Act at sections 5, 10, 13-17, 22 and within the HPPs in Schedule 1.

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

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

18. Before completing the review, check whether the Privacy Commissioner wishes to make a submission. Ideally you should provide a draft copy of your preliminary determination to the Privacy Commissioner for comment. At the very least you are required to provide the Privacy Commissioner with the findings of the review and the action your agency proposes to take (s54(1)(c)).

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

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

- Alleged conduct occurred; the conduct did not comply with the IPPs/public register provisions; the non-compliance was not authorised ('a breach').

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

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

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

☐ Yes - go to Q.22

☐ No - go to Q.21

b) Did the agency breach an HPP?

☐ Yes - go to Q.22

☐ No - go to Q.21

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

☐ Yes – go to Q.22

☐ No – go to Q.24

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

☐ Apology to complainant

☐ Rectification to complainant, e.g.:

☐ Access to their personal information or health information

☐ Correction of their personal information or health information

☐ Other type of rectification

☐ Expenses paid to complainant

☐ Compensatory damages paid to complainant

☐ Other remedy to complainant

☐ Review of policies, practices or systems

☐ Change in policies, practices or systems

☐ Training (or further training) for staff

☐ Other action

☐ No action

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

☐ Yes

☐ No

☐ Unsure

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

- that you have completed the Internal Review;
- what your findings are, i.e. which one of the following:
- insufficient evidence to suggest alleged conduct occurred
- alleged conduct occurred but complied with the IPPs/public register provisions
- alleged conduct occurred; did not comply with the IPPs/public register provisions; but non-compliance authorised by an exemption, Code or s.41 Direction
- alleged conduct occurred; the conduct did not comply with the IPPs/public register provisions; the non-compliance was not authorised ('a breach')
- what the reasons for your findings are;
- a plain English explanation of the law behind your findings, including quoting in full the relevant legislative provisions you are talking about;
- what action/s you are going to take as a result;
- that the complainant has the right to apply to the Tribunal within 28 days[1] for a review of the conduct complained about; and
- the contact details for the Tribunal.

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

- that you have completed the Internal Review;
- what your findings are, i.e. which one of the following:
- insufficient evidence to suggest alleged conduct occurred
- alleged conduct occurred but complied with the HPPs
- alleged conduct occurred; did not comply with the HPPs; but non-compliance authorised by an exemption, Code, or

s.62 Direction

- alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised ('a breach')
- what the reasons for your findings are;
- a plain English explanation of the law behind your findings, including quoting in full the relevant legislative provisions you are talking about;
- what action/s you are going to take as a result;
- that the complainant has the right to apply to the Tribunal within 28 days[2] for a review of the conduct complained about, and
- the contact details for the Tribunal.

25. Keep a record of this review for your annual reporting requirements

For more information

Contact the Information and Privacy Commission

NSW (IPC): Freecall: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au

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