information and privacy commission
new south wales

Privacy Internal Review Guidelines

May 2025

Contents

Glossary

CEO	Chief Executive Officer of the NSW Information and Privacy Commission
HPPs	The Health Privacy Principles established under the *Health Records and Information Privacy Act 2002*. There are 15 HPPs set out in Schedule 1 of the Act
HRIP Act	*Health Records and Information Privacy Act 2002* (NSW)
ICAC	Independent Commission Against Corruption
IPC	The Information and Privacy Commission NSW (IPC) is an independent statutory authority that oversees legislation dealing with privacy and access to government held information in New South Wales.
IPPs	The Information Protection Principles established under the *Privacy and Personal Information Protection Act 1998.* There are 12 IPPs set out in Part 2, Division 1 of the Act.
NCAT	NSW Civil and Administrative Tribunal. An applicant may apply to the NCAT to appeal a privacy internal review decision made by the IPC.
PCO	Privacy Contact Officer at the IPC is the Director, Corporate Services and Business Improvement
PPIP Act	*Privacy and Personal Information Protection Act 1998* (NSW)

Introduction and Acknowledgment

It is important that privacy concerns are appropriately managed by the IPC. A prompt and respectful response to individuals who raise privacy complaints about the way the IPC as an agency has handled personal information is an important aspect of maintaining public confidence and trust in the IPC.

The aim of these guidelines is to support IPC staff to comply with all legislative requirements in conducting privacy internal reviews. These guidelines apply when the IPC undertakes a privacy internal review in accordance with NSW privacy legislation. The IPC Privacy Policy, Privacy Management Plan, Code of Conduct, and Service Charter should also be considered and where relevant applied when managing corporate privacy matters. The IPC acknowledges that these Privacy Internal Review Guidelines are a modified version of the NSW Health Privacy Internal Review Guidelines (2019) and consent has been received by NSW Health for their use and publication.

Part 1	Provides an overview of the legislative framework for privacy internal review and the role of the Privacy Contact Officer.
Part 2	Addresses the application for privacy internal review, including what determines a valid application and the time limit for submitting an application.
Part 3	Provides guidance on the conduct of the privacy internal review, including conducting interviews and consultation requirements.
Part 4	Addresses the drafting of the privacy internal review report.
Part 5	Explains the applicant's right to appeal, annual reporting requirements and the role of the NSW Privacy Commissioner.
Parts 6 and 7	Provide references, pro forma letters, templates and a flow chart to assist the review officer to meet legislative requirements when conducting a privacy internal review.

Part 1 - Background

1.1 NSW privacy laws

NSW privacy laws govern the management of personal information held by public sector agencies in NSW. The two NSW privacy laws are:

- *Health Records and Information Privacy Act 2002 (NSW)* (HRIP Act)
- *Privacy and Personal Information Protection Act 1998 (NSW)* (PPIP Act)

The HRIP Act governs health information that may include personal information. The PPIP Act governs all other 'non-health' personal information. In IPC, this mostly comprises employee records. The PPIP Act sets out 12 Information Protection Principles. The IPC Privacy Management Plan provides guidance on how to comply with the requirements of the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs). The provisions for privacy internal review are set out in Part 5 of the PPIP Act. These provisions apply to privacy internal reviews of alleged breaches under both the HRIP Act and the PPIP Act. These guidelines reflect these legislative provisions.

1.2 When is internal review required?

A request for a privacy internal review can be made where an individual believes that the IPC has:

- breached any of the HPPs
- breached any of the IPPs
- breached any code of practice or public interest direction made under either Acts applying to the IPC
- disclosed information on a public register, except in accordance with section 57 of the PPIP Act only.

If the IPC receives a complaint from an individual who is aggrieved by the handling of their personal or health information, the IPC is required to consider whether to undertake a privacy internal review. A privacy internal review must be conducted if the complaint is in the form of a valid application (see section 2.1).

An individual may also complain on behalf of someone else if they are authorised to act on their behalf. In these cases, the authorisation must be checked to determine its application (e.g. to whom is it granted), its scope (e.g. what functions does it authorise the nominated individual to undertake), and its duration (e.g. is it current and operative in respect of the date of the authority). In addition, an individual may be aggrieved by the handling of someone else's personal or health information and such a complaint may also require a privacy internal review (see section 2.2).

Often the individual's initial complaint will not be in the form of a privacy internal review application. Nonetheless, if an individual expresses dissatisfaction with the handling of their personal or health information, the IPC must provide the person with information on their right to request a privacy internal review, and the requirements for lodging a valid application.

1.3 When is internal review not required?

There may be circumstances where internal review is not the appropriate response when an individual raises privacy concerns. Examples include:

- A person may raise general concerns about the systems for handling information of the IPC. The IPC may wish to address the person's concerns by reference to information management policies rather than through a privacy internal review process.

- A client may express concern about the access controls relating to their case management record. The client may be satisfied with an explanation about the operational policies for access controls over IPC records.

In these scenarios, privacy internal review may not be the appropriate response. Either the information does not relate to the individual making the complaint, the person is not aggrieved by the handling of their information, or the complainant does not want a privacy internal review.

1.4 Chief Executive Officer, NSW Privacy Commissioner and Privacy Contact Officer roles

The IPC's CEO is ultimately responsible for the handling of a privacy complaint about the IPC. The CEO is required to nominate a person to act as Privacy Contact Officer (PCO) for the IPC. The CEO or their delegate, other than the PCO or Review Officer, should approve the final privacy internal review report before the report is sent to the applicant. The IPC's PCO is responsible for overseeing privacy complaints, including privacy internal reviews, in accordance with these guidelines and their contact details are on the IPC Website.

The NSW Privacy Commissioner has a monitoring and oversight role during the course of an internal review. When an application for internal review is received, the IPC should:

- notify the Privacy Commissioner of the application as soon as practicable (see Appendix 6)
- keep the Privacy Commissioner informed of the progress of the internal review
- inform the Privacy Commissioner of the draft findings of the review and of the action proposed to be taken by the IPC in relation to the matter (see Appendix 7).

The IPC should not release the findings of the privacy internal review to the applicant until the IPC has received any submissions or comments from the Privacy Commissioner as this might lead to the report's amendment Generally, the Privacy Commissioner requires a minimum of two weeks to review and respond to a draft report. The Privacy Commissioner can sometimes be delayed. If this happens it is important to keep the applicant informed of the delay.

If the Privacy Commissioner's comments or submissions are delayed, the applicant should be advised via the standard extension letter (see Appendix 5.3).

It is usual practice for the PCO to conduct the internal review, unless the PCO has a conflict of interest or is otherwise directed by the CEO. Should an officer other than the PCO be nominated to conduct the privacy internal review, they may be referred to as the Review Officer for the purposes of conducting the review.

The PCO must also keep statistical data about the number of internal review requests received. Staff should consult with the PCO regarding privacy queries and complaints they receive about breaches of privacy.

Privacy related complaints may also be part of a governance related complaint made to another business unit within the IPC. Similarly, an Internal Audit may become aware of privacy issues during audits or other investigations. When identified, issues should be referred to the PCO for consideration.

The CEO is responsible for ensuring that a framework is in place to manage privacy training for staff. The framework or training register should ensure that all staff undertake the mandatory privacy training modules, and that all staff with access to information systems have been appropriately trained and understand their privacy obligations as IPC employees in accordance with the IPC's Code of Conduct.

1.5 Informing the public about privacy internal review

The IPC informs the public about its privacy policies and procedures, including how to make a privacy complaint and the process of internal review. The IPC achieves this by publication on its website of privacy related policies and procedures.

Requests for information about the internal review process should be directed to the IPC's PCO or CEO. A pro forma Information Sheet, which includes information about the requirements for requesting an internal review, is set out in Appendix 3.

Part 2 - The application

2.1 A valid privacy internal review application

Part 5 of the PPIP Act requires that an application for internal review must:

- be in writing
- be addressed to the agency (i.e. the IPC)
- specify an address in Australia to which the applicant is to be notified after the completion of the review
- be lodged at an office of the agency within 6 months from the time the applicant first became aware of the conduct. The agency may allow an extension of time in special circumstances (discussed below in section 2.4).

2.2 Applicant must be aggrieved

An application for internal review can only be made by a person who is "aggrieved" by the conduct of the IPC in relation to their information privacy, or by an authorised representative of that aggrieved person.

An aggrieved person can be someone other than the individual to whom the information relates. For example, a parent of a child might be aggrieved about a breach of their child's privacy, or a person might be aggrieved about a breach of their elderly parent's privacy. Sometimes a third party can also be affected by a disclosure.

Where the applicant is not the individual to whom the information relates, the IPC should assess the application to identify if this person has been directly affected by the alleged breach.

Consideration should then be given to what extent, if any, it would be appropriate to provide information about the client to the applicant.

2.3 Internal review application form

The IPC Privacy Internal Review Application Form is provided in Appendix 4.

It is not obligatory for applicants to complete a form. It is sufficient for their complaint to be received in writing (e.g. letter or email). However, the application form can be useful for both the applicant to articulate their complaint and for the IPC to gain a more detailed understanding of the complaint.

Therefore, this form should be provided to applicants where possible. A pro forma letter requesting completion of the form is provided at Appendix 5.1.

The PCO should always contact the complainant prior to initiating an internal review, to ensure that all issues that may assist the internal review have been identified.

2.4 Extension of 6-month time limit

An application for privacy internal review must be lodged within 6 months from the time the applicant first became aware of the conduct which their complaint relates to. If the time frame is over six months, the application is considered 'out of time'. If the date at which the applicant became aware of the conduct which is the subject of the complaint is unclear in the application, clarification should be sought from the applicant before proceeding with any aspect of the internal review process.

The IPC may exercise its discretion to extend the time for receiving internal review applications beyond the 6-month period. In determining whether to accept an application made after the 6- month period, the IPC may consider:

- the length of the delay
- the merits of the complaint
- whether the complainant can demonstrate a reasonable explanation for the delay, such as ill health, family trauma or other reasons relating to incapacity.

An applicant should always be offered the opportunity to explain the delay before a decision is reached to decline an application. This will be relevant in circumstances where the applicant's complaint has been received via an email or letter instead of the IPC privacy internal review application form (which provide the applicant with an opportunity to explain any delay).

If an applicant has not provided a reason for the delay, they do not need to be provided with another opportunity to explain the delay and it can be presumed there is no reasonable explanation. On this basis, a decision not to extend time can be made by the IPC.

Any decision to extend time for an applicant should be made in consultation with the CEO.

If a decision is made not to extend the time for receiving the application beyond the 6-month period, the IPC should inform the individual of this decision. A pro forma letter is provided at Appendix 5.2.

The IPC's response to the applicant will vary depending on the circumstances.

In most circumstances, the IPC's Privacy Contact Officer will undertake an assessment of the concerns raised by the complaint to determine whether any management action should be taken in response. The complainant would normally be informed of the outcome of such an assessment.

Where the complaint is not privacy related, or includes other matters, it should be referred to the appropriate complaint handling staff of the IPC or other authorities as appropriate.

2.5 Anonymised applications for internal review

In some circumstances, an applicant may want their letter of complaint or internal review application anonymised when it is provided to the Privacy Commissioner. The Privacy Contact Officer should carefully review the application to assess whether there is any indication that anonymity should be preserved. While an internal review can be completed this way, the applicant should be informed that disclosure of their personal details will be required if they wish to apply for a further review by the NSW Civil and Administrative Tribunal (NCAT).

If the applicant and witnesses are anonymised in the internal review, their identities should be documented by the IPC in its internal file notes.

For example:

John Brown – The Applicant

Sarah Clarke – Witness A

2.6 Recordkeeping

All documents received and created in relation to internal review applications will be stored in the IPC's secure electronic document management system with appropriate security controls.

Part 3 – Conducting the privacy internal review

3.1 Review officer

The privacy internal review must be conducted by an officer who, as far as practicable:

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

In most cases, the review officer will be the IPC's PCO. A person may be considered substantially involved if they had direct or indirect knowledge of the matter prior to receiving the privacy complaint or were in any way involved in or responsible for the conduct which led to the complaint. This includes involvement in attempts to informally resolve the complaint. In complaints such as these, the PCO should declare a conflict of interests and recuse themselves from any review of the matter.

Where the PCO is unable to undertake the privacy internal review, the CEO must appoint another internal officer capable of undertaking a fair and unbiased internal review, in accordance with these guidelines. Where difficulties arise, guidance can be sought from the Privacy Contact Officer, to assist in selecting a suitable review officer.

The PPIP Act allows for the agency to request that the NSW Privacy Commissioner undertake a privacy internal review. However, in practice, it would be extremely unlikely for the Privacy Commissioner to undertake this role, given that in relation to an IPC service, IPC staff provide support services to the Privacy Commissioner to fulfill their statutory functions

3.2 60-day time limit to complete the review

The review officer must complete the review as soon as reasonably practicable in the circumstances, and in any event within 60 calendar days from the day on which the complaint was received. The Act allows an additional 14 days for the IPC to notify the applicant of the findings and recommendations, in exceptional cases. The 60-day time limit starts from the receipt of the first written privacy complaint or request for privacy internal review, regardless of whether an application form is used.

To ensure completion of the internal review within this time limit, the review officer should prepare a work plan that allocates sufficient time over the 60-day period for all steps involved, including:

- 1 to 2 weeks for gathering and reviewing documents and interviewing the applicant and individuals who can assist with providing information for the review.
- 1 week to prepare the draft report, including the review of relevant records, and reference to relevant policy and procedures.
- 1 week for consideration of the draft report by the Director, Regulatory Advice & General Counsel.
- 1 week for consideration of the draft report by the CEO
- 2 weeks for consideration of the draft report by the Privacy Commissioner,
- 1 week to amend the draft in response to feedback from the Privacy Commissioner.

Provision of the final report to the applicant must be within the 60-day time period, unless permission is obtained from the applicant to extend. In exceptional cases, an additional 14 days may be allowed for postage.

3.3 Reviews not completed within 60 days

The review must be completed as soon as is reasonably practicable in the circumstances. If the IPC foresees that completion of the review will take longer than 60 calendar days, the review officer should advise the applicant in advance, explaining why 60 days was insufficient in the circumstances, and inform the applicant of the expected completion date.

If the review has not been completed within 60 calendar days, the applicant is entitled to make an application to the NCAT for a review of the conduct concerned. The applicant must be informed of this when they are advised of any delay on the completion of the report. See the pro forma letter at Appendix 5.3.

3.4 Acknowledging receipt of application

When an internal review application is received by the IPC, it must be promptly forwarded to the IPC's PCO for review.

As soon as practicable after receiving the application, , the review officer should acknowledge receipt of the application and if necessary, gather further information about the nature of the complaint. This can be particularly useful if the applicant has only provided brief comments as part of the standard application form. It will also assist the review officer to identify which privacy principles may have been breached and provide an opportunity to manage the applicant's expectations.

Where the applicant has provided sufficient detail in their application to undertake an internal review, a letter of acknowledgement of their application should be sent and the internal review commenced. A pro forma letter acknowledging receipt of the completed form is provided at Appendix 5.1.

3.5 Notifying the Privacy Commissioner

The PCO or Review Officer will advise the Privacy Commissioner that an application for internal review has been received, and provide a copy of the application. The application form allows the applicant to withhold identifying information from the Privacy Commissioner. See Appendix 6 for a pro forma letter of notification to the Privacy Commissioner.

3.6 Steps in an internal review

An internal review may involve:

- seeking further information from the applicant
- reviewing internal IPC records or other documents held relevant to the application
- referring to IPC policies and relevant local procedures to determine whether staff involved in the complaint acted in accordance with these policies and procedures
- interviewing staff or other individuals involved in the conduct which is the subject of the complaint
- checking with the applicant as to whether other privacy complaints have been made to the IPC. Any prior complaints regarding the same matter should be documented in the internal review report as background.

3.7 Procedural fairness

Procedural fairness must be afforded to staff who are the subject of the internal review.

Information must be provided to the staff member about the complaint and any allegations made against him or her. The review officer should also explain the review process to the staff member. Information about the complaint should be detailed enough to allow the staff member to provide a considered response. If the person is to be interviewed, the person should be provided at least 48 hours' notice.

Procedural fairness requires that a person the subject of review must be given an opportunity to respond to adverse findings made against them before any disciplinary action is taken. The review officer must act impartially and without bias.

As in all matters, care must be taken to maintain confidentiality of the applicant and third parties involved in the matter.

The final internal review report should not be provided to the staff member who is the subject of the complaint. However, the staff member should be permitted to review and comment on any statements attributed to them or transcripts from records of interview. If necessary, a staff member may review excerpts of a draft report, to verify factual matters.

Affected staff should also be informed about any adverse findings relevant to them. In the event that multiple staff have been interviewed for an internal review, care needs to be taken to ensure the confidentiality of each staff member is respected and maintained.

In some matters, particularly if it is likely that disciplinary action may be taken, the reviewer should consult with the CEO before liaising with the People and Culture branch in the Department of Customer Service (IPC's service provider) during the review process. See below at section 3.12.

For further information, see the following resources from the NSW Ombudsman:

Good conduct and administrative practice - Guidelines for state and local government

3.8 Interviewing the applicant – where necessary

Interviewing the applicant can be of great assistance to clarify the precise nature of the concerns held by the applicant. Often applicants can better explain their complaint verbally than in writing. In most cases it will be beneficial to interview the applicant in person where the PCO identifies that this would assist in clarifying the issues of concern. All attempts to contact the applicant should be documented.

It can be useful to prepare a list of questions to ask the applicant at the interview. Key issues to consider when interviewing the applicant include:

- Does any of the information in the application require clarification?
- Is any information missing?
- What other information do we need to collect as part of a diligent review?
- Are there individuals inside or outside the IPC who should be contacted about the complaint? How can they be contacted?
- Has the applicant already complained about the conduct before submitting their application for internal review? If so, to whom was the complaint made and what was the response?

During the interview, the review officer should explain to the applicant the actions that can be taken by the IPC to resolve the applicant's concerns. Manage the applicant's expectations – explore what outcome they are seeking, then indicate what action may be taken by the IPC. Explain that proper process must be followed, including an explanation of the process for an internal review.

3.9 Interviewing others

In addition to the applicant, the review officer should also consider conducting interviews with:

- the staff member who is the subject of the complaint
- all other relevant staff members
- in rare circumstances, other clients or members of the public who may have witnessed or been involved in the incident that gave rise to the complaint.

Interviews can be conducted in person or by telephone. A staff member who is the subject of a complaint should be advised of the nature of the complaint, the internal review process and any relevant evidence Once the internal review report has been finalised, the staff member should be advised of the findings. This is particularly important if their conduct is being referred to the CEO for disciplinary management.

Staff who are interviewed should review any records of interview or statements to ensure that they accurately reflect their version of events. This is important if the applicant appeals to NCAT, because staff will need to prepare affidavits detailing their version of events.

Under the IPC Code of Conduct it is expected that staff will assist in the interview process. If a person does not agree to participate in an interview, discuss with the People and Culture branch.

If relevant staff have left the organisation, and they are important witnesses, they may be invited to participate in an interview. However, caution should be exercised, and this should only be done with the approval of a senior officer.

In some circumstances staff may want their identities to be anonymous in the report. For example, this might be because:

- the applicant or the applicant's family have made threats of violence to the staff member
- the report raises workplace relations issues
- staff reside in small rural communities
- the applicant is a staff member.

Advice on anonymising staff identities can be sought from the PCO. Occasionally, clients or other members of the public may also be approached as witnesses. Consideration should be given as to whether contacting these individuals is reasonable having regard to the seriousness of the complaint and how long ago the events occurred. Any decisions that are made about how to proceed and the reasons for those decisions should be documented in a file note and retained as part of the internal review file.

Sometimes the applicant may be opposed to involving other people who may have information that would assist the review. If the review officer believes that approaching these individuals would assist in confirming a breach of privacy, it should be explained to the applicant that if the individuals are not contacted it may affect the outcome of the review. If the applicant insists that they not be contacted, this should be documented in the internal review report, so it is clear to the NSW Privacy Commissioner why certain aspects of the complaint were not investigated by the IPC.

Members of the public are not obliged to assist in an internal review and their participation is voluntary. All attempts to approach members of the public should be documented. It is recommended that advice from a senior executive be sought prior to initiating such contact.

If a member of the public does not agree to participate in the internal review, their identity should be anonymous in the internal review report. However, the personal details of potential witnesses should be recorded separately, so that they can be contacted if their information later becomes relevant to NCAT proceedings.

3.10 Has the IPC breached a privacy principle?

In light of the information gathered through the internal review, the review officer must identify which Health Privacy Principles (HPPs) under the HRIP Act, or Information Protection Principles (IPPs) under the PPIP Act have been breached. Where it is suspected that a staff member has breached an IPP, the review officer must determine the nature and extent of the breach including if it was deliberate or accidental.

The review officer may wish to consult with the Privacy Contact Officer to ensure the correct privacy principles have been identified.

Issues that may require consideration include:

- Was the personal or information used or disclosed without authority?
    - HPPs 10/11 and IPPs 10/11
- Would the applicant have a reasonable expectation that their information would be used by the IPC in this way?
    - HPP 10 and IPP 11
- What evidence is there that the applicant was informed about the use of their information?
    - HPP 4 and IPP 3
- Was the applicant given appropriate access to their records?
    - HPP 7 and IPP 7
- Was the applicant aware that their personal or information was being collected?
    - HPP 4 and IPP 3
- If not, was the information lawfully collected?
    - HPP 1 and IPP 1
- Is the information held about the applicant accurate?
    - HPP 9 and IPP 9
- Was the information held securely?
    - HPP 5 and IPP 5

3.11 Has the privacy of other persons been breached?

In some circumstances, an application for privacy internal review may raise system failures or breaches that may impact on the privacy of persons other than the applicant. Any data breaches raised in an application, must be reported by the review officer in accordance with the IPC's Data Breach Policy and relevant legislation.

3.12 Referral for Disciplinary Action?

If the concerns raised in the application are likely to warrant the staff member's referral for disciplinary action, the review officer should raise this with the CEO, or as soon as this becomes apparent.

3.13 Does the matter raise a public interest disclosure?

An intentional breach of privacy made by an employee may amount to a privacy contravention under the *Public Interest Disclosures Act 2022*. The review officer should ensure that a matter that is, or appears to be, a public interest disclosure, is handled in accordance with the IPC's Public Interest Disclosures policy.

3.14 Is consultation required with NSW Police?

Criminal offences in the HRIP Act, PPIP Act and/or the *Crimes Act 1900* may apply to staff for unauthorised access to, or misuse of, information.

There are statutory time limits that may impact on these complaints. It is very important that they are reported to NSW Police and that the Privacy Commissioner is notified as soon as possible.

Section 308H of the *Crimes Act 1900* provides for an offence for unauthorised access to or modification of restricted data held in a computer. Proceedings for an offence against section 308H must be commenced **within 12 months** from when the offence was alleged to have been committed.

Most other summary offences (including the offences relating to corrupt disclosure or misuse of information under the HRIP Act and PPIP Act) must be prosecuted **within 6 months** of the offence.

Applicants need to be made aware of their rights to make a complaint to police before these time periods expire. Applicants should be advised to seek independent legal advice in relation to pursuing a prosecution.

In these circumstances, the Privacy Contact Officer must notify the CEO immediately to ensure reporting to external bodies can take place in a timely manner.

Part 4 – The internal review report

4.1 Content of the report

Appendix 8 provides an Internal Review Report template to assist in the writing of the report.

The report must include:

- Background information on the facts and history of the complaint. A timeline that summarises the sequence of events may be helpful.. Make sure relevant policies and procedures are clearly set out.
- A description of the review process (for example, list of interviewees, documents, records and policies referenced). Describe the approach taken to analyse the information and evidence that has been collected.
- The findings of the review including whether a privacy breach was found to have occurred, and the reasons for those findings. The report should clearly demonstrate to the applicant and the Privacy Commissioner how the reviewer has come to make the findings.

The findings should address whether more could have been done by the IPC to prevent a privacy breach occurring. Questions to consider may include:

- Were the IPC's practices compliant with IPC policy and legislative requirements?
- Has the IPC implemented sufficient data security safeguards?
- Have staff received appropriate privacy training?
- Are audits conducted of staff access to electronic medical records?
- The recommendations of the review and the reasons for these recommendations.
- The right of the person to have the findings and the IPC's proposed actions reviewed by the NSW Civil and Administrative Tribunal (NCAT).

The report must recommend one or more of the following:

- Make a formal apology to the applicant (if a breach has been substantiated this should always occur)
- Take such remedial action as the review officer thinks appropriate (for example, provide compensation to the applicant, amendment of records)
- Provide undertakings that the conduct will not occur again
- Implement administrative measures to ensure that the conduct will not occur again, such as revision of relevant policies and guidelines, introduction of new business rules or systems, and privacy training for relevant staff
- Take no further action on the matter (if no breach has been substantiated).

The report may include recommendations in relation to referral to Internal Audit or another body for further assessment. The report should not make a finding of criminal or corrupt conduct. However, if there is a concern that any conduct may be criminal in nature the report should make a recommendation that the matter be referred to Internal Audit or another body to assess whether the conduct should be reported to ICAC or police.

Points to consider when writing the report:

- Use plain language and avoid jargon and acronyms as far as possible.
- The report should be helpful to the applicant, and provide open and transparent explanations of the circumstances surrounding the complaint
- The report will be sent to the applicant, so care must be taken not to disclose personal information about any third parties
- Any information provided on behalf of staff members should be accurate and consistent with their statements.
- If the applicant disagrees with the findings of the review, he or she may appeal to NCAT. If there is an appeal, the internal review report will be submitted as evidence to NCAT, so it is essential that it reflects that a fair, unbiased, thorough and accurate review has taken place.
- Reference should be made to policies, procedures, records of signed privacy undertakings, privacy training records, audit reports, client information leaflets and any other documents relevant to the circumstances of the complaint. This helps to clarify how personal information is managed by the IPC system. For example, it may be useful to explain to an applicant the security measures in place to prevent unauthorised access to information, including the signed undertakings and individual personal logins that are required.

4.2 Review of draft report by Director, Regulatory Advice & General Counsel

The Review Officer will provide a copy of the draft report to the Director, Regulatory Advice & General Counsel.

4.3 Review of draft reports by the CEO and Privacy Commissioner

The draft report is to be provided to the CEO for any feedback prior to referring the draft report to the Privacy Commissioner.

The PPIP Act requires the Privacy Commissioner to be kept informed of the progress of the internal review and to inform the Privacy Commissioner of the review findings and the action proposed to be taken in response to the findings. The Privacy Commissioner is entitled to make submissions (discussed at section 4.4) in relation to the application.

See Appendix 7 for a pro forma letter / email providing the draft internal review report to the Privacy Commissioner.

4.4 Submissions from the Privacy Commissioner

Any submissions received from the Privacy Commissioner should be taken into consideration when preparing the final report.

4.4 Issuing the final report

Following completion of the review, the IPC must provide the applicant with the completed Internal Review Report and covering letter (Appendix 5.4) as soon as practicable or, in any event, within 14 days of completion (section 53(8) of the PPIP Act). However, if there are extenuating circumstances and the report cannot be provided within the required timeframe, the officer should contact the applicant, explain the circumstances for the delay and request additional time to complete the review (see the pro forma extension of time letter, Appendix 5.3).

The IPC must notify the applicant in writing of:

- the findings of the review and the reasons for those findings
- the action proposed to be taken by the IPC and the reasons for taking that action
- the right of the person to have those findings, and the IPC's proposed action, reviewed by the NCAT.

A copy of the final Internal Review Report and covering letter sent to the applicant must be provided to the Privacy Commissioner.

Part 5 – Appeals, annual reporting, and role of the Privacy Commissioner

5.1 Appeals to the NSW Civil and Administrative Tribunal

If the applicant is dissatisfied with the outcome of the internal review, the applicant has a right to appeal to the NCAT within 28 calendar days from being notified of the findings of the internal review.

If the appeal deadline has passed, the applicant can ask NCAT for an extension. It will be up to NCAT to decide whether or not to accept a late application.

As the case proceeds through NCAT process from planning meetings and case conferences to the hearing date, the parties may attempt to resolve the complaint through negotiation.

If the case proceeds to a hearing, NCAT may make one or more of the following orders after the hearing is completed:

(a) An order requiring the IPC to pay to the applicant damages not exceeding $40,000 by way of compensation for any loss or damage suffered because of the conduct.

(b) An order requiring the IPC to refrain from any conduct or action in contravention of an information protection principle or a privacy code of practice.

(c) An order requiring the performance of an information protection principle or a privacy code of practice.

(d) An order requiring personal information that has been disclosed to be corrected by the IPC.

(e) An order requiring the IPC to take specified steps to remedy any loss or damage suffered by the applicant.

(f) An order requiring the IPC not to disclose personal information contained in a public register.

(g) Such ancillary orders as NCAT thinks appropriate.

Alternatively, NCAT may decide not to take any further action on the matter.

5.2 Annual reporting

The IPC must include certain privacy-related information in its annual report pursuant to Division 7.3 of the *Government Sector Finance Act 2018*. In accordance with TPG23-10 *Annual Reporting Requirements*, the annual report must include:

- a statement of the action taken by the IPC in complying with the requirements of the PPIP Act, such as the delivery of privacy training to staff and distribution of information regarding privacy to clients
- statistical data on any privacy internal reviews conducted by or on behalf of the IPC.

The report should provide details of when the applications for review were received, and a summary of the outcomes. The summary should include:

- whether any privacy principles were breached, and the broad context of the breach;
- whether the applicant sought further review in NCAT and a summary of any NCAT findings.

Care must be taken to ensure that the details included in the annual report in no way identify the applicant or other participants in the internal review.

5.3 Role of the Privacy Commissioner

Investigating privacy complaints

Privacy complaints about a public sector agency, including about the IPC, can also be made to the Privacy Commissioner (under section 45 of the PPIP Act).

Part 6 – References

6.1 Legislation

Privacy and Personal Information Protection Act 1998 (NSW)

Health Records and Information Privacy Act 2002 (NSW)

6.2 IPC

Privacy Contact Officer email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au/privacy

IPC Privacy Management Plan

IPC Code of Conduct

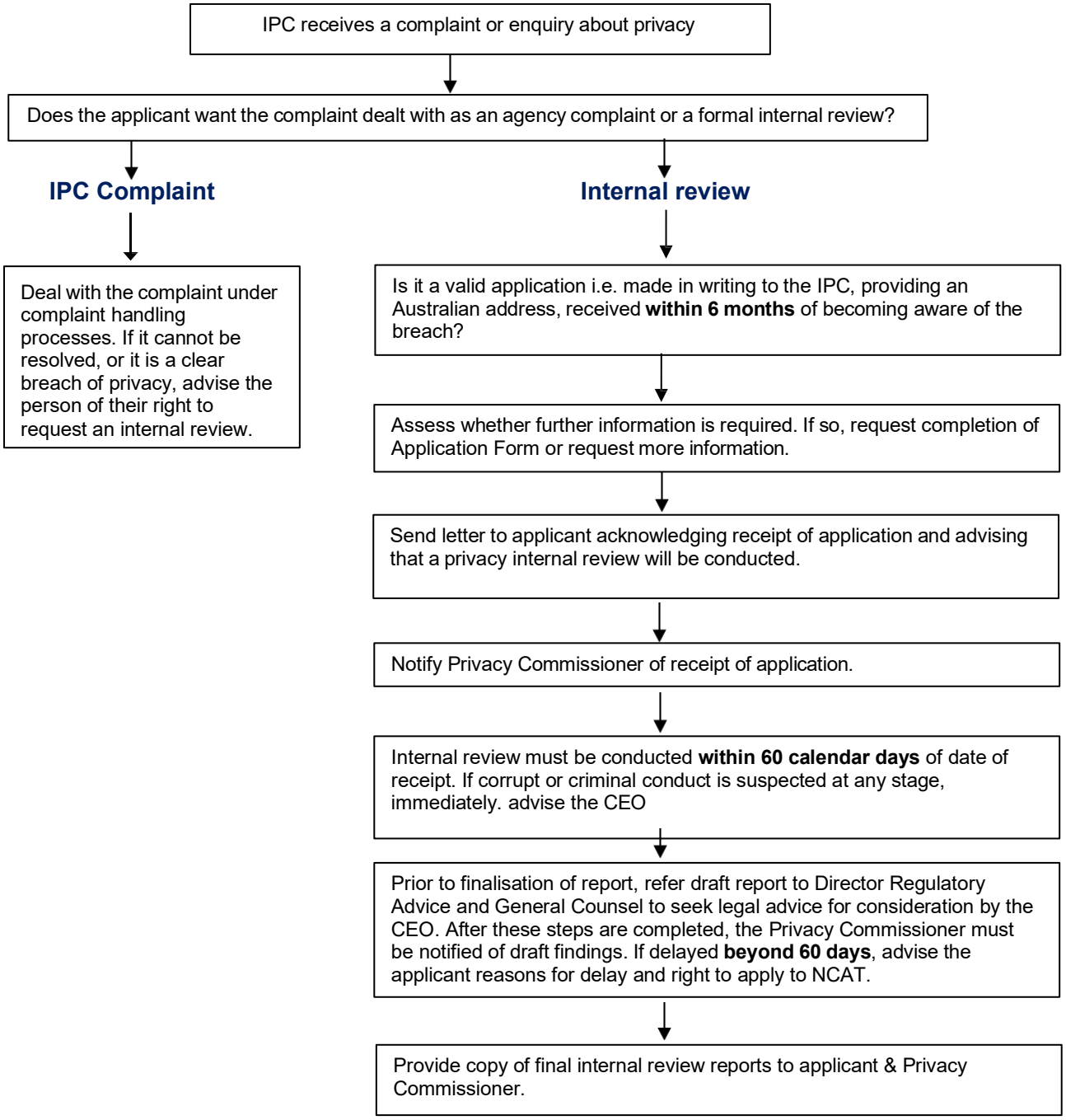
Internal Review Checklist for the Respondent Agency

Protocol for handling privacy complaints

Resources for public sector agencies

Part 7 – Appendices

Appendix 1 – Flowchart of the internal review process



Appendix 2 – Checklist for privacy internal review

1. Preliminary steps

a) Is the complaint about a person's personal information?

☐ Yes – you should treat their complaint as a request for Internal Review.

☐ 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.

b) 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 over the page.

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.

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.

c) According to the complainant, when did the alleged conduct occur?

_____

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

_____

e) When was this application / privacy complaint first lodged?

_____

Note: In Y v DET, the Administrative Decisions Tribunal 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.

f) If more than six months lapsed between the date of the alleged conduct and when the complaint was lodged, decide whether to accept a late application.

Will you accept this late application?

☐ Yes – continue to Step 1 g

☐ 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.

g) When will 60 days elapse from the date of receiving the application?

_____

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 internal 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.

h) For complaints about a person's personal information, not including health information, tick all of the following types of conduct that describe the complaint.

☐ 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.

i) 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.)

j) Insert the reviewing officer's name here:

_____

k) 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 s53(4) of the PPIP Act. This also applies to the HRIP Act.)

l) Write to the complainant, stating:

- your understanding of the conduct complained about
- your understanding of the privacy principle/s at issue (either IPPs or HPPs noted above)
- 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
- that if your review is not complete by the date at Step 1g 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
- that notice of your application and the subject matter of the application s54 PPIP will be provided to the Privacy Commissioner for their oversight role.

Note: s54 of the PPIP Act requires the agency to:

1. *notify the Privacy Commissioner that it has received the application*
2. *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.*

m) Send notice of the application to the Privacy Commissioner (s54 PPIP Act).

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

2. You can now start the review itself

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)
- 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 s41 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
- 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 s62 Direction from the Privacy Commissioner.

3. On completion of the review

a) Under the PPIP Act, you need to make a determination on:

- whether the alleged conduct occurred
- if so, whether the conduct complied with all the IPPs (and Part 6 public register provisions if applicable)
- 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 s41 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 under the PPIP Act and are published on the IPC website. Section 41 Directions only modify the IPPs, not the public register provisions. Directions are published on the IPC website.

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

- whether the alleged conduct occurred
- if so, whether the conduct complied with all the HPPs
- 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.

Before completing the review, you should send a draft copy of your report (prior to finalisation) to the Director, Regulatory Advice and General Counsel to obtain legal advice for the consideration of the CEO. After making amendments to the draft report following the CEO's review, the draft report must be provided to the Privacy Commissioner for comment, and to determine whether the Commissioner wishes to make a submission.

c) Under the PPIP Act, finalise your determination of the internal review, by making one of the following findings against each allegation:

- 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').

d) 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').

e) Have you identified any need for improvement in policies, procedures, communicating with clients, etc?

_____

f) What action is proposed as a result of this review? (You can have more than one)

- ☐ Apology to complainant, rectification to complainant
- ☐ 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

g) Is the proposed action likely to match the expectations of the complainant?

- ☐ Yes
- ☐ No
- ☐ Unsure

h) Under the PPIP Act, notify the complainant and the Privacy Commissioner in writing:

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

- what action/s you are going to take as a result
- that the complainant has the right to apply to the Tribunal within 28 days1 for a review of the conduct complained about
- the contact details for the Tribunal.

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

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

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

[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

Appendix 3 – Information for privacy internal review

Privacy internal review is a process through which the IPC handles complaints about how it has dealt with personal information under the NSW *Privacy and Personal Information Protection (PPIP) Act 1998* and personal information under the *Health Records and Information Privacy (HRIP) Act 2002*.

Individuals have the right to seek an internal review of certain conduct of the IPC, in circumstances where the individual believes that the IPC has breached the terms of either the PPIP Act and / or the HRIP Act.

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

- breached any of the Information Protection Principles under the PPIP Act, and/ or any of the Health Privacy Principles under the HRIP Act that apply to the IPC
- breached any code made under the Acts applying to the IPC
- disclosed personal information or personal information kept in a public register.

Please see IPC fact sheet on How to handle an Internal Review.

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

- the findings of the review and the reasons for those findings
- the action proposed to be taken by the IPC including the reasons for taking that action
- the right of the applicant to have the findings of the review and proposed action of the IPC reviewed by the NSW Civil and Administrative Tribunal (NCAT).

If an applicant is not satisfied with the findings of the internal review, or the action taken by the IPC in relation to the application, or the application is not decided within 60 days, the applicant may apply to NCAT for a review of the conduct that was the subject of the application. The application to NCAT must be made within 28 calendar days from being notified of the findings of the internal review.

Appendix 4 – Privacy internal review application form

This is an application form for review of conduct under:

- s53 of the NSW *Privacy and Personal Information Protection Act 1998* (the PPIP Act)
- s21 of the IPC *Records Information Privacy Act 2002* (the HRIP Act)

Find the online webform here: Privacy complaint internal review application form.

Appendix 5 – Letters to the applicant

Letters to the applicant may vary depending on the information provided in the initial application and other factors. The following templates may be adapted for use:

- **Appendix 5.1** Acknowledgement of receipt of application
- **Appendix 5.2** Letter to the applicant advising the application is out of time
- **Appendix 5.3** Letter to the applicant requesting an extension of time to complete the review.

Once the internal review report has been finalised and any submissions made by the Privacy Commissioner have been considered, the IPC should send a copy of the internal review report to the applicant under the cover of the following letter:

- **Appendix 5.4** Letter to the applicant – Completed internal review report.

Appendix 5.1 – Acknowledgement of receipt of application

[Date]

APPLICANT'S NAME
APPLICANT'S ADDRESS Our ref:

Dear APPLICANT'S NAME

RE: Application for privacy internal review

I wish to acknowledge receipt of your application for privacy internal review by the Information and Privacy Commission NSW (IPC) on the [date].

In my role as Privacy Contact Officer and being independent of the circumstances surrounding your complaint, I will conduct this internal review for the IPC. Your application will be reviewed having regard to the requirements of the *Health Records and Information Privacy Act 2002* [*if information*] OR the *Privacy and Personal Information Protection Act 1998* [*if personal information*]. *[Optional, if the applicant has not completed a privacy internal review application form:* Please find enclosed the IPC privacy internal review application form. While it is not required, we would appreciate it if you could complete and return this form as soon as possible. It will assist us in better understanding your complaint.]

Under the law, the IPC is allowed 60 calendar days to conduct the internal review from the day on which the application was received. As we received your application on [*date*], we will complete your internal review by [*date*]. We will contact you if for any reason the internal review has not been finalised by this date and explain the circumstances for the delay. Alternatively, if the internal review is not completed within 60 days, you may apply directly to the NCAT for an administrative review. The contact details for the Tribunal are:

NSW Civil & Administrative Tribunal

Registry Administrative & Equal Opportunity Division

Level 10 John Maddison Tower 86-90 Goulburn Street

Sydney NSW 2000

Telephone: **1300 006 228**

Online at: www.ncat.nsw.gov.au

The law requires that the Privacy Commissioner be notified of this application and be advised of the progress of the review. A copy of your application has been forwarded to the Privacy Commissioner. [Delete this sentence if the applicant indicates they want to be anonymous. In such cases, a deidentified copy of the application should be provided to the Privacy Commissioner with the applicant's consent]

If you have any questions relating to this matter, please do not hesitate to contact me on [telephone number and email details].

Yours sincerely

Name of Privacy Contact Officer/ Review Officer

Appendix 5.2 – Letter to the applicant advising the application is out of time

[Date]

APPLICANT'S NAME
APPLICANT'S ADDRESS Our ref:

Dear APPLICANT'S NAME

RE: Your application for privacy internal review

In reference to your letter and application for privacy internal review dated XXXXX, it is noted that you became aware of the alleged conduct which is the subject of the complaint on XX/XX/20XX.

Section 53 of the *Privacy and Personal Information Protection Act 1998* states an application for a review of conduct must 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 which is the subject of the application.

It is noted that your complaint is outside of the six-month time limit, being approximately X months/ years since the date you became aware of the alleged conduct.

[*Optional, if the application appears to have substance and the applicant has not completed an IPC standard privacy internal review application form*:]

In order for us to consider whether to accept your application outside of the six-month period, please provide us with your reasons for the delay in submitting the application (e.g. ill health, family trauma or other reasons). Your reasons should be provided to me by email or letter within 7 days.

[If the applicant completed a standard internal review application form but failed to provide sufficient reasons for delay beyond 6 months]:

As your application has not provided sufficient reasons to justify an extension of this time period, the Information and Privacy Commission NSW (IPC) is declining to accept your application for internal review and will not conduct an internal review pursuant to NSW privacy laws.

However, the IPC will consider the issues raised by your complaint as part of our normal administrative processes.

I appreciate that this decision may cause you some concern and you are welcome to contact me. If you have any questions relating to this decision please contact me on *[telephone number and email details].*

Yours sincerely

Privacy Contact Officer / Review Officer

Appendix 5.3 – Letter requesting an extension of time to complete the review

[Date]

APPLICANT'S NAME
APPLICANT'S ADDRESS Our ref:

Dear APPLICANT'S NAME

RE: Extension of time to complete privacy internal review

I refer to your application for a privacy internal review by the Information and Privacy Commission NSW (IPC) received on [*date*]. As you are aware, the *Privacy and Personal Information Protection Act 1998* allows the IPC 60 days to conduct the internal review from the day on which the application was received. This review was due to be completed on or before the [*date*].

It is regrettable that due to [*describe the circumstances*], I have not been able to complete your internal review and sincerely apologise for the delay. However, as discussed in our telephone conversation [*or via email*], I would like to request that an extension be granted so that the review can be appropriately completed. I anticipate that the review will be completed by [*date*]. If there is to be any further delay, I will contact you prior to this revised completion date.

Given that the internal review was not completed within 60 days and you will not be provided with the outcome of review on time, you are entitled to make an application under section 55 of the *Privacy and Personal Information Protection Act 1998* to the NSW Civil and Administrative Tribunal for an administrative review of the conduct concerned. The contact details for the Tribunal are:

NSW Civil & Administrative Tribunal

Registry Administrative & Equal Opportunity Division

Level 10 John Maddison Tower 86-90 Goulburn Street

Sydney NSW 2000

Telephone: **1300 006 228**

Online at: www.ncat.nsw.gov.au

If you await the completion of the internal review, you are still entitled to seek a review of the conduct in the NSW Civil and Administrative Tribunal and you will be further advised of this when the internal review is completed.

If you have any questions relating to this matter, please don't hesitate to contact me on [*telephone number and email details*].

Yours sincerely

Privacy Contact Officer / Review Officer

Appendix 5.4 – Letter to the applicant – Completed internal review report

[Date]

APPLICANT'S NAME
APPLICANT'S ADDRESS Our ref:

Dear [NAME OF APPLICANT],

RE: Outcome of your application for privacy internal review

I write to you in reference to your complaint dated [*date*] addressed to the [*name of officer and* Information and Privacy Commission *who have received the complaint*]. In summary, your complaint concerned [*briefly summarise nature of complaint in neutral terms*].

An internal review of the circumstances surrounding your complaint has been carried out in accordance with the *Health Records and Information Privacy Act 2002* [*if dealing with personal information]* OR the *Privacy and Personal Information Protection Act 1998* [*if dealing with personal information]*. As required by the Act, I have notified the NSW Privacy Commissioner of your privacy complaint. A copy of this notification is enclosed.

The details of the internal review are provided in the attached report. In summary, it is found that a breach of privacy principles in relation to your health / OR personal/ information has/ OR has not occurred. [*List the specific issues and summary of findings*]

If you are dissatisfied with the outcome of this review, the Act provides you with a right to lodge an appeal to the NSW Civil and Administrative Tribunal within 28 calendar days from receipt of this correspondence (+ 5 calendar days for postage). The Tribunal's contact details are:

NSW Civil and Administrative Tribunal

Registry Administrative & Equal Opportunity Division

Level 10 John Maddison Tower 86-90 Goulburn Street

Sydney NSW 2000

Telephone: **1300 006 228**

Online at: www.ncat.nsw.gov.au

If you require any additional information in relation to the internal review conducted in accordance with [*the Health Records and Information Privacy Act 2002* or the *Privacy and Personal Information Protection Act 1998]*, please contact [*name*], Privacy Contact Officer, NSW Information and Privacy Commission on [*telephone number and email details*].

Yours sincerely

Privacy Contact Officer / Review Officer

Enclosed - Copy of letter of notification to Privacy Commissioner
- Privacy Internal Review Report

Appendix 6 – Letter to Privacy Commissioner notifying receipt of application

[Date]

[Name of Privacy Commissioner]
Privacy Commissioner Our ref:

Via email: ipcinfo@ipc.nsw.gov.au

Dear *[Name of Privacy Commissioner]*

RE: Application for Internal Review by *[Name of applicant]*

This is to advise that an application for an internal review was received by the Information and Privacy Commission NSW *on [*date*].* It will be reviewed having regard to the requirements of the *Health Records and Information Privacy Act 2002* and/or *Privacy and Personal Information Protection Act 1998*.

As the Act allows the IPC 60 calendar days to conduct the internal review from the day on which the application was received, the IPC must complete the review by [*date*].

A copy of the application is attached for your reference. [*Note*: ensure the application is de-identified if requested by the applicant].

When the review is completed, I will provide you with a copy of the draft internal review report for your consideration.

I recognise that under section 54(2) of the *Privacy and Personal Information Protection Act 1998*, you are entitled to make submissions on the subject matter of the application. Any advice you wish to provide on this matter would be appreciated.

I am happy to discuss any aspects of this matter and can be contacted on [*telephone number and email details*].

Yours sincerely

Privacy Contact Officer / Review Officer

Appendix 7 – Letter to Privacy Commissioner providing draft report

[Date]

[Name of Privacy Commissioner]
Privacy Commissioner Our ref:

Via email: ipcinfo@ipc.nsw.gov.au

Dear *[Name of Privacy Commissioner]*

RE: Draft Internal Review Report for *[Name of applicant]*

Please find attached the draft Internal Review Report for the application for internal review received by us from [*name of applicant*].

You were previously notified of the details of this review in our letter, dated [*date*]. Under the *Privacy and Personal Information Protection Act 1998*, the review must be completed by the Information and Privacy Commission NSW by [*date*]. I would appreciate any comments your office may wish to make by [*date*] to allow finalisation of the review within the prescribed time frame.

I am available to discuss any aspects of this matter and can be contacted on [*provide telephone and email details*].

Yours sincerely

Privacy Contact Officer / Review Officer

Appendix 8 – Template for privacy internal review report

REPORT OF INTERNAL REVIEW UNDER THE PRIVACY AND PERSONAL INFORMATION PROTECTION ACT (PPIP ACT) 1998 / HEALTH RECORDS AND INFORMATION PRIVACY ACT (HRIP ACT) 2002 [delete as appropriate]

BACKGROUND

This internal review arises out of an application by [*name of applicant*], ("the applicant").

Once you have written the applicant's name here once, the applicant should be referred to as "the applicant" for the rest of the document. This helps to distinguish the applicant from any witnesses and makes the report easier to read. It also makes it easier to de-identify the report should this be required.

The application relates to events that took place at [describe location] on [describe time frame].

Set out the background which led to the application. This might include a summary of what has occurred, and in more complex cases a detailed chronology of events as determined by the review. Be mindful not to repeat details provided in Section 2. Depending on the nature of the issues raised by the application and the relevance of the circumstances surrounding the complaint, this section could be a very short summary, or quite lengthy.

APPLICATION FOR INTERNAL REVIEW

Summarise:

when application was received

when letter of receipt was sent to the applicant when Privacy Commissioner was advised when internal review was commenced chronology of relevant events.

INTERNAL REVIEW

(Standard Text)

Two pieces of privacy legislation operate in NSW. The *Health Records and Information Privacy Act 2002* (HRIP Act) regulates "information" through 15 Health Privacy Principles (or HPPs). The *Privacy and Personal Information Protection Act 1998* (PPIP Act) regulates general personal information (other than information) through 12 Information Protection Principles and also regulates the review of conduct by public sector agencies for both Acts.

Section 21 of the HRIP Act and section 52 of the PPIP Act allow the following conduct to be subject to an internal review:

a) *the contravention by a public sector agency of an information protection principle/health privacy principle [delete as appropriate] that applies to the agency,*

b) *the contravention by a public sector agency of a privacy code of practice that applies to the agency,*

c) *the disclosure by a public sector agency of personal information kept in a public register.*

In this case, the Review has identified that the application relates to category (a)/(b)/(c) [delete as appropriate].

Before considering the application, a number of preliminary questions must be considered.

Is the information in question "personal information" and/or "information"?

Section 5 of the HRIP Act and section 4 of the PPIP Act defines "personal information" 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"

Determine whether the application relates to "personal information" and indicate briefly why.

Section 6 of the HRIP Act defines "information", including as follows:

(a) personal information that is information or an opinion about:

(i) the physical or mental health or a disability (at any time) of an individual, or

(ii) an individual's express wishes about the future provision of IPCs to him or her, or

(iii) the IPC provided, or to be provided, to an individual, or

(b) other personal information collected to provide, or in providing, the IPC.

Determine whether the application relates to "personal information" and indicate briefly why. State your conclusion:

The appropriate privacy law to be considered is therefore the PPIP Act/HRIP Act [delete as appropriate] and the IPPs/HPPs [delete as appropriate].

Does the applicant have standing to make an application?

Ensure that the person making the application is a person "who is aggrieved by the conduct of a public sector agency" in accordance with section 53 of the PPIP Act

Where the applicant is a person other than the person to whom the information relates, identify why they are considered to be "aggrieved"

What is the conduct relevant to this Review?

Identify the conduct which is subject to the review. This can be done by reference to the application itself or other clarifying material the applicant has provided. It may be helpful to quote relevant sections of the complaint.

ALLEGED BREACHES OF THE PPIP ACT / HRIP ACT [delete as appropriate]

List and summarise each of the Information Protection Principles / or Health Privacy Principles identified as relevant, and again quote sections of the complaint relevant to each principle. Then under 'Assessment of conduct' identify whether the NSW Information and Privacy Commission's conduct has breached each Principle. For example:

Terms of Information Protection Principle or Health Privacy Principle

Insert actual wording of Privacy Principle (or refer to wording in an Attachment).

Assessment of conduct

Summarise outcome of review, refer to policies, client leaflets and other relevant documents considered and identify whether the conduct in question has/has not breached the relevant privacy principle.

Set out information about the review process and analysis of the information and evidence that has been collected, addressing the following:

- *Did the conduct occur and what is the evidence showing this?*
- *If it is found that the conduct did occur, describe how the conduct amounts to a breach of an IPP/HPP.*
- *Where no breach is found, describe how the conduct demonstrates compliance with privacy principles. Refer to IPC's privacy policies. What is the extent of the breach? Consider the seriousness.*

What is an appropriate response in light of a breach?

This assessment should provide relevant information such as dates, information obtained during the course of the review such as audit reports, records of interview that includes factual accounts from individuals, any other supporting documents and records such as privacy undertakings. It is important to note that supporting documents should also include any information that demonstrates that a breach did not occur.

If the evidence of the breach is ambiguous, an assessment can be made as to whether on the balance of probabilities the facts have been established. A fact is proved on the balance of probabilities if its existence is more probable than not. For example, the report might state:

On the balance of probability, it has been determined that details of the applicant's information were / were not disclosed by X to Y without the applicant's consent.

Conclude with the finding:

It is found that this Information Protection Principle / Health Privacy Principle has / has not been breached.

[REPEAT FOR EACH PRINCIPLE IDENTIFIED ABOVE]

FINDINGS

Summarise findings, for example:

The findings of this internal review conclude that there has/ has not been a breach of the Information Protection Principle(s)/ or Health Privacy Principle(s) identified by the applicant which have been the subject of this review.

Where there has been a breach of one or more of the Principles, identify which Principle(s).

The report should clearly demonstrate to the applicant and the Privacy Commissioner how the reviewer has come to make the findings. This requires reference to information gathered in the internal review and how it establishes compliance or non-compliance with the IPPs/HPPs.

RECOMMENDATIONS

(Standard Text)

Section 53(7) of the PPIP Act sets out the list of possible recommendations that may be provided at the end of the internal review. These are to:

- take no further action on the matter make a formal apology to the applicant
- provide undertakings that the conduct will not occur again
- implement administrative measure to ensure that the conduct will not occur again (for example, revision of relevant policies and guidelines, and privacy training for relevant staff)
- take such remedial action as it thinks appropriate.

In this case, the applicant has sought:

Identify what the applicant has asked to occur, irrespective of whether it falls within the above categories.

Set out the recommendations arising out of the review. In doing so, have regard to what the applicant has asked for and the list of possible recommendations listed in the PPIP Act. If the review does not propose to act on the applicant's request(s), explain why in a neutral manner.

Response to applicant's request for monetary compensation

In circumstances where an applicant requests money (for example, as compensation for a breach or for reimbursement of costs incurred as a result of a breach), the following approach is suggested:

In this case, the applicant has sought:

Identify what the applicant has asked to occur.

If the report has identified that a breach has not occurred, then your recommendations would not include any offer of compensation, damages or reimbursement of costs.

If the report has identified that a breach of privacy has occurred and the applicant has requested compensation, then you may invite provision of evidence to substantiate a claim, for example:

Your request for compensation is noted. Since the internal review has identified that your privacy has been breached, you may be eligible for compensation.

Compensation can only be provided in limited circumstances, for example, if you have suffered loss or damage (financial, psychological or physical) as a direct result of the breach of privacy.

If you consider you are eligible for compensation you can write to the Information and Privacy Commission NSW directly outlining the compensation you believe you are entitled to receive. You should attach receipts if you have them. The Information and Privacy Commission NSW will then contact its insurer and seek an early evaluation of your claim.

As outlined in the covering letter, if you are dissatisfied with the Information and Privacy Commission's response, the Act provides you with a right to lodge an appeal to the NSW Civil and Administrative Tribunal within 28 calendar days from receipt of this correspondence (+ 5 calendar days for postage).

There are maximum financial limits for compensation claims. For more information, please refer to information on the IPC Website.

Document information

Identifier/Title:	Privacy Internal Review Guidelines
Business Unit:	IPC
Author:	Manager, Systems and Corporate Services
Approver:	Director, Corporate Services and Business Improvement
Date of Effect:	May 2025
Next Review Date:	May 2026
EDRMS File Reference:	D25/016455/DJ
Key Words:	Privacy, Guidelines, PPIP Act, Review