

PRIVACY NSW – COMPLAINTS TO PUBLIC SECTOR AGENCIES

INTERNAL REVIEW CHECKLIST FOR THE RESPONDENT AGENCY

The *Privacy and Personal Information Protection Act 1998* (the PPIP Act) and the *Health Records and Information Privacy Act 2002* (the 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).¹

A privacy complaint may come under:

- the PPIP Act, section 53,² 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).

	Steps to follow	Date completed
	Preliminary steps	
1	<p>Is the complaint about a person's personal information?³</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes – You should treat their complaint as a request for Internal Review. Go to Q.2. <input type="checkbox"/> No – Follow your agency's normal complaint handling procedures. 	
2	<p>Is the complaint about a person's health information?⁴</p> <ul style="list-style-type: none"> <input type="checkbox"/> 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. Go to Q.3. <input type="checkbox"/> 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. Go to Q.3. <input type="checkbox"/> Both – See the notes below.⁵ Go to Q.3. 	
3	According to the complainant, when did the alleged conduct occur?	
4	<p>Is the complaint about conduct that occurred after 1 July 2000?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes – Go to Q.5. <input type="checkbox"/> No – The PPIP Act does not apply. Follow your agency's normal complaint handling procedures. 	
5	<p>Is the complaint about health information and conduct that occurred after 1 September 2004?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes – the HRIP Act covers this complaint. Go to Q.6. <input type="checkbox"/> No – the PPIP Act covers this complaint. Go to Q.6 	
6	According to the complainant, when did they first <i>become aware</i> of the alleged conduct? ⁶	
7	When was this application / privacy complaint first lodged? ⁷	

8	<p>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.⁸</p> <p>Will you accept this late application?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes – Go to Q.9. <input type="checkbox"/> No – Explain your reasons to the complainant, then follow your agency’s normal complaint handling procedures. 	
9	<p>When will 60 days elapse from the date at Q.7?</p> <p><i>After this date the complainant may go to the Administrative Decisions Tribunal (‘the Tribunal’) without waiting for the results of this review.</i></p>	
10	<p>For complaints about a person’s health information go to Q.11</p> <p>For complaints about a person’s personal information, not including health information, tick all of the following types of conduct⁹ that describe the complaint. Then go to Q.12.</p> <ul style="list-style-type: none"> <input type="checkbox"/> collection of the complainant’s personal information (IPPs 1-4) <input type="checkbox"/> security or storage of the complainant’s personal information (IPP 5) <input type="checkbox"/> refusal to let the complainant access or find out about their own personal information (IPPs 6-7) <input type="checkbox"/> accuracy or relevance of the complainant’s personal information (IPPs 8-9) <input type="checkbox"/> use of the complainant’s personal information (IPP 10) <input type="checkbox"/> disclosure of the complainant’s personal information (IPPs 11-12, and/or the public register provisions in Part 6 of the Act) <input type="checkbox"/> other / it’s not clear 	
11	<p>For complaints about a person’s health information, tick all of the following types of conduct¹⁰ which describe the complaint:</p> <ul style="list-style-type: none"> <input type="checkbox"/> collection of the complainant’s health information (HPPs 1-4) <input type="checkbox"/> security or storage of the complainant’s health information (HPP 5) <input type="checkbox"/> refusal to let the complainant access or find out about their own health information (HPPs 6-7) <input type="checkbox"/> accuracy or relevance of the complainant’s health information (HPPs 8-9) <input type="checkbox"/> use of the complainant’s health information (HPP 10) <input type="checkbox"/> disclosure of the complainant’s health information (HPP 11) <input type="checkbox"/> assignment of identifiers to the complainant (HPP 12) <input type="checkbox"/> refusal to let the complainant remain anonymous when entering into a transaction with your agency (HPP 13) <input type="checkbox"/> transfer of the complainant’s health information outside New South Wales (HPP 14) <input type="checkbox"/> including the complainant’s health information in a health records linkage system (HPP 15) <input type="checkbox"/> other / it’s not clear 	
12	<p>Appoint a reviewing officer. <i>(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.)</i></p> <p>Insert the reviewing officer’s name here:</p>	

13	<p>Write to the complainant, stating:</p> <ul style="list-style-type: none"> <input type="checkbox"/> your understanding of the conduct complained about, <input type="checkbox"/> your understanding of the privacy principle/s at issue (either IPPs at Q.10 or HPPs at Q.11), <input type="checkbox"/> that the agency is conducting an Internal Review under the PPIP Act or the HRIP Act, as appropriate, <input type="checkbox"/> the name, title, and contact details of the reviewing officer, <input type="checkbox"/> how the reviewing officer is independent of the person/s responsible for the alleged conduct, <input type="checkbox"/> the estimated completion date for the review process, <input type="checkbox"/> 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 <input type="checkbox"/> that a copy of this letter will be provided to the NSW Privacy Commissioner for their oversight role. 		
14	<p>Send a copy of your letter at Q.13 to the NSW Privacy Commissioner, at GPO Box 6, Sydney NSW 2001; or fax (02) 9228-8577.</p> <p>If the complainant has consented,¹¹ include a copy of the complainant's application – either the whole application or just the information provided at Q's 5-12 on the <i>Privacy Complaint: Internal Review Application Form</i>.</p>		
Now you can start the review itself			
15	<p><u>Under the PPIP Act</u></p> <p>You need to determine:</p> <ul style="list-style-type: none"> <input type="checkbox"/> whether the alleged conduct occurred, <input type="checkbox"/> if so, whether the conduct complied with all the IPPs (and Part 6 public register provisions if applicable)¹², and <input type="checkbox"/> if the conduct did not comply with an IPP (or the public register provisions), whether the non-compliance was authorised by: <ul style="list-style-type: none"> <input type="checkbox"/> an exemption under the PPIP Act¹³, <input type="checkbox"/> a Privacy Code of Practice¹⁴, or <input type="checkbox"/> a s.41 Direction from the Privacy Commissioner.¹⁵ 	<p><u>Under the HRIP Act</u></p> <p>You need to determine:</p> <ul style="list-style-type: none"> <input type="checkbox"/> whether the alleged conduct occurred, <input type="checkbox"/> if so, whether the conduct complied with all the HPPs¹⁶, and <input type="checkbox"/> if the conduct did not comply with an HPP, whether the non-compliance was authorised by: <ul style="list-style-type: none"> <input type="checkbox"/> an exemption under the HRIP Act¹⁷, <input type="checkbox"/> a Health Privacy Code of Practice¹⁸, or <input type="checkbox"/> a s.62 Direction from the Privacy Commissioner.¹⁹ 	
16	<p>Four weeks after sending the letter at Q.13, send a progress report to the complainant and the Privacy Commissioner.²⁰ Include:</p> <ul style="list-style-type: none"> <input type="checkbox"/> details of progress of the review, <input type="checkbox"/> if there are delays, an explanation of this and a revised estimated completion date for the review process, and <input type="checkbox"/> 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. 		

On completion of the review		
17	<p><u>Under the PPIP Act</u></p> <p>Write up your findings about the facts, the law, and your interpretation of the law.</p> <p>Set out your preliminary determination about:</p> <ul style="list-style-type: none"> <input type="checkbox"/> whether there was sufficient evidence to establish that the alleged conduct occurred, <input type="checkbox"/> which of the IPPs (and/or the public register provisions) you examined and why, <input type="checkbox"/> whether the conduct complied with the IPPs/ public register provisions, <input type="checkbox"/> if the conduct did not comply with an IPP or public register provision, whether the non-compliance was authorised by: <ul style="list-style-type: none"> <input type="checkbox"/> an exemption under the PPIP Act, <input type="checkbox"/> a Privacy Code of Practice, or <input type="checkbox"/> a s.41 Direction from the Privacy Commissioner, and <input type="checkbox"/> an appropriate action for the agency by way of response/ remedy. 	<p><u>Under the HRIP Act</u></p> <p>Write up your findings about the facts, the law, and your interpretation of the law.</p> <p>Set out your preliminary determination about:</p> <ul style="list-style-type: none"> <input type="checkbox"/> whether there was sufficient evidence to establish that the alleged conduct occurred, <input type="checkbox"/> which of the HPPs you examined and why, <input type="checkbox"/> whether the conduct complied with the HPPs, <input type="checkbox"/> if the conduct did not comply with an HPP, whether the non-compliance was authorised by: <ul style="list-style-type: none"> <input type="checkbox"/> an exemption under the HRIP Act, <input type="checkbox"/> a Health Privacy Code of Practice²¹, or <input type="checkbox"/> a s.62 Direction from the Privacy Commissioner²², and <input type="checkbox"/> an appropriate action for the agency by way of response/ remedy.
18	<p>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.</p>	
20	<p><u>Under the PPIP Act</u></p> <p>Finalise your determination of the Internal Review, by making one of the following findings:</p> <ul style="list-style-type: none"> <input type="checkbox"/> insufficient evidence to suggest alleged conduct occurred <input type="checkbox"/> alleged conduct occurred but complied with the IPPs/ public register provisions <input type="checkbox"/> 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 <input type="checkbox"/> alleged conduct occurred; the conduct did not comply with the IPPs/ public register provisions; the non-compliance was not authorised (“a breach”) 	<p><u>Under the PPIP Act</u></p> <p>Finalise your determination of the Internal Review, by making one of the following findings:</p> <ul style="list-style-type: none"> <input type="checkbox"/> insufficient evidence to suggest alleged conduct occurred <input type="checkbox"/> alleged conduct occurred but complied with the HPPs <input type="checkbox"/> alleged conduct occurred; did not comply with the HPPs; but non-compliance was authorised by an exemption, Code or s.62 Direction <input type="checkbox"/> alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised (“a breach”)
21	<p>Did the agency breach an IPP or public register provision?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes – Go to Q.23. <input type="checkbox"/> No – Go to Q.22 	<p>Did the agency breach an HPP?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes – Go to Q.23. <input type="checkbox"/> No – Go to Q.22

22	<p>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 your clients, etc?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes – Go to Q.23. <input type="checkbox"/> No – Go to Q.25. 	
23	<p>What action is proposed by the agency as a result of this review? <i>(You can have more than one.)</i></p> <ul style="list-style-type: none"> <input type="checkbox"/> apology to complainant <input type="checkbox"/> rectification²³ to complainant, eg: <ul style="list-style-type: none"> <input type="checkbox"/> access to their personal information or health information <input type="checkbox"/> correction of their personal information or health information <input type="checkbox"/> other type of rectification <input type="checkbox"/> expenses paid to complainant <input type="checkbox"/> compensatory damages paid to complainant <input type="checkbox"/> other remedy to complainant <input type="checkbox"/> review of policies, practices or systems <input type="checkbox"/> change in policies, practices or systems <input type="checkbox"/> training (or further training) for staff <input type="checkbox"/> other action <input type="checkbox"/> no action 	
24	<p>Is the proposed action likely to match the expectations of the complainant?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unsure 	

25	<p><u>Under the PPIP Act</u></p> <p>Notify the complainant and the Privacy Commissioner²⁴ in writing:</p> <ul style="list-style-type: none"> <input type="checkbox"/> that you have completed the Internal Review, <input type="checkbox"/> what your findings are, i.e. which one of the following: <ul style="list-style-type: none"> <input type="checkbox"/> insufficient evidence to suggest alleged conduct occurred <input type="checkbox"/> alleged conduct occurred but complied with the IPPs/ public register provisions <input type="checkbox"/> alleged conduct occurred; did not comply with the IPPs/ public register provisions; but non-compliance authorised by an exemption, Code or s.41 Direction <input type="checkbox"/> alleged conduct occurred; the conduct did not comply with the IPPs/ public register provisions; the non-compliance was not authorised ("a breach") <input type="checkbox"/> what the reasons for your findings are, <input type="checkbox"/> a plain English explanation of the law behind your findings, including quoting in full the relevant legislative provisions you are talking about, <input type="checkbox"/> what action/s you are going to take as a result, <input type="checkbox"/> that the complainant has the right to apply to the Tribunal for a review of the conduct complained about, and <input type="checkbox"/> the contact details for the Tribunal. 	<p><u>Under the HRIP Act</u></p> <p>Notify the complainant and the Privacy Commissioner²⁵ in writing:</p> <ul style="list-style-type: none"> <input type="checkbox"/> that you have completed the Internal Review, <input type="checkbox"/> what your findings are, i.e. which one of the following: <ul style="list-style-type: none"> <input type="checkbox"/> insufficient evidence to suggest alleged conduct occurred <input type="checkbox"/> alleged conduct occurred but complied with the HPPs <input type="checkbox"/> alleged conduct occurred; did not comply with the HPPs; but non-compliance authorised by an exemption, Code, or s.62 Direction <input type="checkbox"/> alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised ("a breach") <input type="checkbox"/> what the reasons for your findings are, <input type="checkbox"/> a plain English explanation of the law behind your findings, including quoting in full the relevant legislative provisions you are talking about, <input type="checkbox"/> what action/s you are going to take as a result, <input type="checkbox"/> that the complainant has the right to apply to the Tribunal for a review of the conduct complained about, and <input type="checkbox"/> the contact details for the Tribunal. 	
26	Keep a record of this review for your annual reporting requirements. ²⁶		

NOTES

¹ 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.

² 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 6 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.*)

³ “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 (eg. 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 Privacy NSW as to the extent to which the exemption applies.

⁴ “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 (eg. 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 Privacy NSW as to the extent to which the exemption applies.

⁵ 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.

⁶ 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 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 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. For more on this issue see the April 2003 *PCO Newsletter*, available on our website via <http://www.lawlink.nsw.gov.au/pc.nsf/pages/generalinfo>

⁹ ‘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.

¹⁰ See footnote 8 above.

¹¹ See Q.14 on the *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 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.

¹³ Exemptions are found in the PPIP Act at sections 4-6, 20, and 23-28.

¹⁴ Privacy Codes of Practice are instruments made by the Attorney General (under the PPIP Act). Many can be found on the Privacy NSW website at: <http://www.lawlink.nsw.gov.au/pc.nsf/pages/codesmade>

¹⁵ Section 41 Directions only modify the IPPs, not the public register provisions. These Directions are usually temporary so check the dates carefully, and contact Privacy NSW for earlier versions of Directions if necessary. All current s.41 Directions can be found at: <http://www.lawlink.nsw.gov.au/pc.nsf/pages/section41orders>.

¹⁶ 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.

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

¹⁸ Health Privacy Codes of Practice are instruments made by the Attorney General (under the HRIP Act). No Health Privacy Codes of Practice have been made to date. To see some Privacy Codes of Practice go to the Privacy NSW website at: <http://www.lawlink.nsw.gov.au/pc.nsf/pages/codesmade>

¹⁹ Section 62 Directions modify the HPPs. These Directions will usually be temporary so check the dates carefully. To date no s.62 Directions have been passed.

²⁰ You are obliged under section 54(1)(b) of the PPIP Act to keep the Privacy Commissioner notified of progress. This also applies to the HRIP Act.

²¹ To date no Health Privacy Codes of Practice have been made.

²² To date no s.62 Directions have been passed.

²³ 'Rectification' means putting things right, the way they should have been in the first place.

²⁴ Sections 53(8) and 54 of the PPIP Act.

²⁵ Sections 53(8) and 54 of the PPIP Act; this also applies to the HRIP Act.

²⁶ The annual report of each public sector agency must include statistical details of any Internal Review conducted: see s.33(3) of the PPIP Act; this also applies to the HRIP Act.