Privacy Internal Review

Checklist

July 2014

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

A privacy complaint may come under:

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

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

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

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

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

Preliminary steps

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

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

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

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

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

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

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

☐ Both – See the notes below.

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

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

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

_____

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

☐ Yes – go to Q.5.

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

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

☐ Yes – the HRIP Act covers this complaint.

☐ No – the PPIP Act covers this complaint.

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

_____

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

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

_____

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

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

Will you accept this late application?

☐ Yes – go to Q.9.

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

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

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

_____

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

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

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

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

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

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

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

12. Insert the reviewing officer's name here:

_____

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

13. Write to the complainant, stating:

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

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

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

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

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

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

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

NSW Privacy Commissioner
GPO Box 7011, SYDNEY NSW 2001

Or fax (02) 8114 3756

or email ipcinfo@ipc.nsw.gov.au

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

You can now start the review itself

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

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

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

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

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

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

On completion of the review

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

☐ Yes - go to Q.22

☐ No - go to Q.21

b) Did the agency breach an HPP?

☐ Yes - go to Q.22

☐ No - go to Q.21

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

☐ Yes – go to Q.22

☐ No – go to Q.24

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

☐ Apology to complainant

☐ Rectification to complainant, e.g.:

☐ Access to their personal information or health information

☐ Correction of their personal information or health information

☐ Other type of rectification

☐ Expenses paid to complainant

☐ Compensatory damages paid to complainant

☐ Other remedy to complainant

☐ Review of policies, practices or systems

☐ Change in policies, practices or systems

☐ Training (or further training) for staff

☐ Other action

☐ No action

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

☐ Yes

☐ No

☐ Unsure

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

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

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

- that you have completed the Internal Review;
- what your findings are, i.e. which one of the following:
- insufficient evidence to suggest alleged conduct occurred
- alleged conduct occurred but complied with the HPPs
- alleged conduct occurred; did not comply with the HPPs; but non-compliance authorised by an exemption, Code, or s.62 Direction
- alleged conduct occurred; the conduct did not comply with the HPPs; the non-compliance was not authorised ('a breach')
- what the reasons for your findings are;
- a plain English explanation of the law behind your findings, including quoting in full the relevant legislative provisions you are talking about;
- what action/s you are going to take as a result;
- that the complainant has the right to apply to the Tribunal within 28 days[2] for a review of the conduct complained about, and
- the contact details for the Tribunal.

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

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au

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