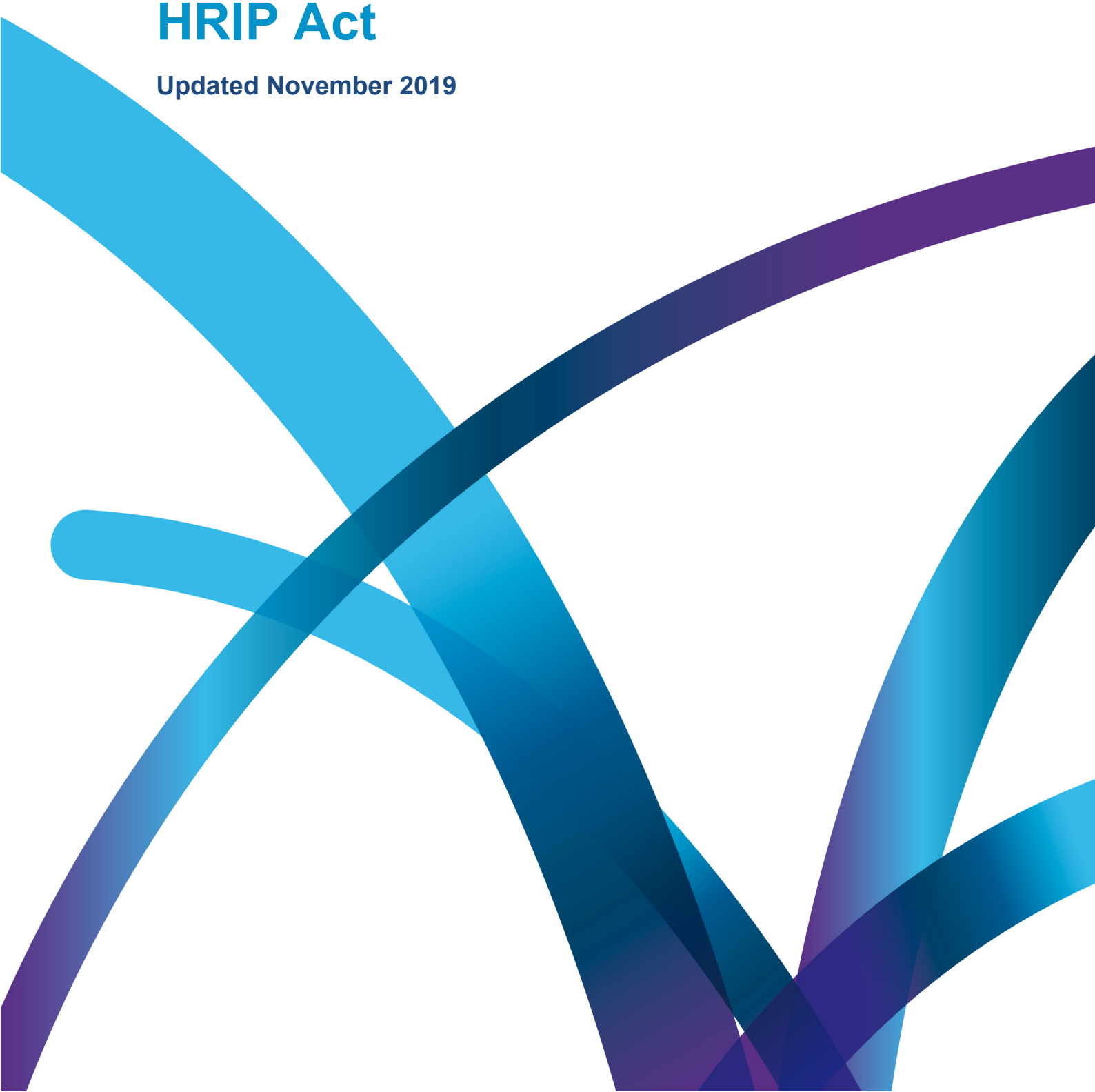
information and privacy commission
new south wales

Guidance on the preparation and assessment of Privacy Codes of Practice under the PPIP Act and HRIP Act

Updated November 2019



Contents

Overview

The purpose of this guidance is to help public sector agencies (and, in the case of health information, public sector agencies and private sector persons) to understand their obligations when seeking a Privacy Code of Practice (Privacy Code) under the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) or the *Health Records and Information Privacy Act 2002* (HRIP Act). This guidance describes the statutory requirements for requesting and making a Privacy Code and the current means by which those Codes are made. It also provides information about the matters which the Privacy Commissioner will take into account when making a submission to the Attorney General or Minister for Customer Service on Privacy Codes, or Health Minister on a Health Privacy Code.

What is a Privacy Code of Practice?

A Privacy Code is a legal instrument made under the PPIP Act or the HRIP Act which modifies an Information Protection Principle (IPP), a PPIP Act public register provision, a Health Privacy Principle (HPP), or a private sector health provision.[1] The Attorney General or Minister makes Privacy Codes by means of an order which is published in the Gazette and which generally takes effect when the order making the Code is published.

A Privacy Code may specify how a principle or provision will apply in a particular circumstance. It may also modify the application of a principle or provision or it may exempt public sector agencies from compliance with a principle.[2] While Privacy Codes must not be more stringent than the privacy protections in those Acts, they should not be seen as a tool for blanket exemptions.[3] A breach of a Privacy Code may give rise to a complaint under the PPIP Act or the HRIP Act.[4]

How is a Privacy Code different to a Public Interest Direction?

A Privacy Code differs from a Public Interest Direction under section 41 of the PPIP Act in that it is made by the Attorney General or Minister for Customer Service in consultation with the Privacy Commissioner in respect of personal information. In respect of a Health Privacy Code, it differs from a Public Interest Direction under section 62 of the HRIP Act, in that it is made by the Health Minister in consultation with the Privacy Commissioner and the Attorney General in respect of health information. A Public Interest Direction is made by the Privacy Commissioner in consultation with the Minister for Customer Service for personal information, and the Health Minister and Attorney General or Minister for Customer Service in respect of health information.

A Privacy Code may modify the application of the IPPs, HPPs or the PPIP Act's Public Register Provisions. A Public Interest Direction may waive or modify the application of the IPPs, HPPs or a Privacy Code, which suggests that Privacy Codes may be more than instruments of exemption.

---

[1] Which are contained in Part 4 of the HRIP Act.

[2] See sections 30 of the PPIP Act and s39 of the HRIP Act.

[3] See sections 29(7) of the PPIP Act and 38(6) of the HRIP Act.

[4] Which in the case of a public sector agency, could mean a complaint to the Privacy Commissioner or an Internal Review application to the agency. See Part 5 of the PPIP Act regarding the Internal Review provisions.

Who may seek a Privacy Code?

Public sector agencies, private sector persons which deal with health information (collectively defined with agencies as organisations[5]) and the Privacy Commissioner may seek a Privacy Code. In some cases multiple agencies have requested Privacy Codes in order to facilitate inter-agency programs which have involved transfers of personal and/or health information. If an agency or an organisation is of the view that it requires a Privacy Code it should first consider whether there is a relevant exception within the principle or provision itself, within Division 3 of part 2 of the PPIP Act or whether the legislation under which it operations permits non-compliance.

In the case of personal information section 25 of the PPIP Act provides that agencies need not comply with an IPP if another law authorises or permits non-compliance. If the agency or organisation is of the view that the practice at issue is not authorised by these exceptions, exemptions or other laws it should then consider whether the practice or function at issue should be provided for by an amendment to the law under which it currently operates. If this is not possible it should then consider whether the practice or function is necessary for the conduct of the agency's or the organisation's business.

It is also possible for agencies or organisations to seek a Privacy Code for the purpose of providing a more practically based and/or a more comprehensive privacy compliance regime with less emphasis on exemption and more on detailed privacy protection. Both the PPIP Act and the HRIP Act provide that Privacy Codes may also "specify requirements that are different from the requirements" set out in the PPIP Act and the HRIP Act or that "specify the manner in which the [privacy] principles may apply".[6] These types of Privacy Codes have been made under the Commonwealth Privacy Act for particular industry groups.[7]

How will the Privacy Commissioner assess a request for a Privacy Code of Practice?

The Privacy Commissioner has the responsibility of making submissions to the Attorney General or Minister for Customer Service and/or the Minister for Health on whether a code should be made.

The stated intention of the PPIP Act is to provide for the protection of personal information and protection of the privacy of individuals generally.[8] The stated intention of the HRIP Act is to protect the privacy of a person's health information held in the public and private sectors.[9] In assessing and making submissions, the Privacy Commissioner has a responsibility to give effect to the intention of the two Acts, and minimise the potential of Privacy Codes to lessen these rights and expectations.

As noted above, the validity of a Privacy Code depends on a number of conditions specified in the two Acts. Privacy Codes are to be made to protect privacy. They must provide standards of privacy protection which operate to protect organisations from any restrictions in relation to the importation of personal information into New South Wales. They are not to impose higher standards on agencies than those set out in the IPPs and HPPs contained in the two Acts.

---

[5] See section 4 of the HRIP Act.

[6] See sections 30(2)(b) and (c) of the PPIP Act and 39(2)(b) and (c) of the HRIP Act.

[7] See https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/

[8] See the long title of the PPIP Act.

[9] See section 3 of the HRIP Act.

In reviewing draft Privacy Codes and making submissions to the Attorney General or Minister for Customer Service and/or Minister for Health as to whether or not to approve a draft Privacy Code, the Privacy Commissioner will consider the following matters:

1. Scope

PPIP Act Privacy Code of Practice[10]

- Does it modify the application of any one or more of the IPPs to any public sector agency?
- Does it modify the application of Part 6 of the PPIP Act to any public sector agency?
- Does it specify the manner in which any one or more of the IPPs are to be applied to, or are to be followed by, the public sector agency?
- Does it exempt a public sector agency, or class of public sector agencies, from the requirement to comply with any IPP?
- Does it clearly indicate the extent of any such modification, specification or exemption?

HRIP Act Privacy Code of Practice[11]

- Does it modify the application of any one or more of the HPPs to any public or private sector person or organisation?
- Does it modify the application of the provisions of Part 4 of the HRIP Act to any private sector person or organisation?
- Does it specify the manner in which any one or more of the HPPs are to be applied to, or are to be followed by, the public or private sector person or organisation?
- Does it exempt a public or private sector person or organisation, or a class of public or private sector persons or organisations, from the requirement to comply with any HPP?
- Does it clearly indicate the extent of any such modification, specification or exemption?

2. Coverage[12]

Does the proposed Privacy Code clearly identify:

- the class of personal information or health information?
- the public or private sector person or organisation, or the class of public or private sector persons or organisations?
- the activity or class of activities in relation to which the code purports to modify the IPPs or HPPs?

[10] Section 30 of the PPIP Act.
[11] Section 39 of the HRIP Act.
[12] Sections 29(5) of the PPIP Act and 38(4) of the HRIP Act.

3. Consistency with the legislative purpose

- Is the proposed Privacy Code made for the purpose of protecting the privacy of individuals?[13]
- Does the proposed Privacy Code maintain standards of privacy protection which will operate to protect organisations from any restrictions in relation to the importation of personal information or health information into New South Wales?[14]
- Does the proposed Privacy Code impose on any organisation requirements that are more stringent (or of a higher standard) than the IPPs or HPPs?[15] If the answer to this is yes, it is likely that this aspect of the code will be struck down.
- Do any provisions of the proposed code purport to modify an applicable exemption?[16] If the answer is 'yes', it is likely that this aspect of the code will be struck down.

4. Public policy issues

- Has the organisation provided a business case that justifies the making of a Privacy Code?
- What are the genuine difficulties the organisation has in complying with the existing principles? Are there alternative solutions available to the organisation which would avoid the need for a code? As a general principle the Privacy Commissioner would prefer agencies to adopt practices which allow them to comply with the IPPs and HPPs or other provisions.
- Does the proposed Privacy Code substantially affect privacy or other interests of an identifiable group of people, if so:
    - is the Privacy Code discriminatory?
    - has there been appropriate consultation with those who the Code might affect?
- What is the time frame envisaged as appropriate? When is a review of the requirement for the Code planned? The Privacy Commissioner will consider if a Privacy Code should only proceed subject to a sunset clause to allow fuller consultation before a final code is made.
- Will the proposed Privacy Code create a precedent for other organisations? The Privacy Commissioner's recommendations will seek to promote the consistent and uniform effects of code provisions. If an exception for a class of information or activity is made for one organisation it may be difficult to argue against the same exception applying to other organisations. The Commissioner will therefore have regard to the potential precedent effects of any exemption proposed for the Privacy Code.
- Are the modifications to the IPPs or HPPs clearly expressed and readily understandable? Privacy Codes should be readily accessible to individual clients, customers and employees who have rights under either or both the PPIP Act and HRIP Act. They should avoid legal technicality and ambiguity or uncertainty as to how the IPPs or HPPs (or other provisions of the relevant Act) are modified.

[13] Sections 29(1) of the PPIP Act and 38(1) of the HRIP Act.
[14] Sections 29(7)(a) of the PPIP Act and 38(6)(a) of the HRIP Act.
[15] Sections 29(7)(b) of the PPIP Act and 38(6)(b) of the HRIP Act.
[16] Sections 29(6) of the PPIP Act and 38(5) of the HRIP Act.

- Is it likely that the Privacy Code will unduly impact on the ability of an aggrieved person to seek review of an organisation's conduct in the NSW Civil and Administrative Tribunal (NCAT)?[17] As a general proposition an exemption drafted as part of a Privacy Code should not be worded so broadly that it prevents the NCAT reviewing conduct of the organisation that may contravene the overall intention of, or breach the spirit of, the relevant privacy principles or provision. Provisions which permit a departure where it is reasonably necessary to fulfil a legitimate function of an organisation will be preferred to provisions which give an absolute exemption, or provisions the exercise of which are wholly dependent on the discretion of the organisation itself.

What are the steps to making a Privacy Code?

PPIP Act Privacy Codes

An agency may initiate a Privacy Code but must consult with the Privacy Commissioner before submitting the draft Code to the Ministers.[18] The IPC has developed a checklist to assist agencies with the process of preparing a Privacy Code. The checklist outlines the preliminary steps an agency should undertake before seeking advice from the IPC.

The Privacy Commissioner may make submissions to the Ministers about the code.[19] After taking the Privacy Commissioner's submissions into consideration the Ministers may decide to make the Privacy Code by making an order to be published in the Gazette.[20] A Code takes effect when the order is published in the Gazette.[21] These procedures apply to any proposed amendment of a Privacy Code.[22]

When an agency consults with the Privacy Commissioner it should provide a business case which includes all the formal code making requirements. It should also canvass the policy matters above, especially those at points 1, 2, 3 and 4.

HRIP Act Privacy Codes

An organisation (which includes agency) may initiate a Health Privacy Code, but it must consult with the Privacy Commissioner before submitting the draft Health Privacy Code to the Health Minister.[23] The Privacy Commissioner may make submissions to the Health Minister about the draft code.[24] After taking the Privacy Commissioner's submissions into consideration the Minister may decide to make the Health Privacy Code by making an order to be published in the Gazette.[25]

---

[17] A matter may proceed to the NSW Civil and Administrative Tribunal (NCAT) for review of an organisation's conduct following either an internal review under Part 5 of the PPIP Act or a complaint to the Privacy Commissioner under Part 6 of the HRIP Act.

[18] Sections 31(1) and 31(2) of the PPIP Act.

[19] Section 31(3) of the PPIP Act.

[20] Sections 31(4) and 31(5) of the PPIP Act.

[21] Section 31(6) of the PPIP Act.

[22] Section 31(7) of the PPIP Act.

[23] Section 40(7) of the HRIP Act.

[24] Section 40(7) of the HRIP Act.

[25] Section 40(7) of the HRIP Act.

A Health Privacy Code takes effect when the order is published in the Gazette.[26] These procedures apply to any proposed amendment of a code.[27]

When an agency consults with the Privacy Commissioner it should provide a business case which includes all the formal Code making requirements. It should also canvass the policy matters above, especially those at points 1, 2, 3 and 4.

Checklist – Preparing a public interest direction or code of practice:
https://www.ipc.nsw.gov.au/node/1536

[26] Section 40(7) of the HRIP Act.
[27] Section 40(7) of the HRIP Act.

Document information

Identifier/Title:	Guidance on the preparation and assessment of Privacy Codes of Practice under the PPIP Act and HRIP Act
Business Unit:	IPC
Author:	Communications and Corporate Affairs
Approver:	Privacy Commissioner
Date of Effect:	N/A
Next Review Date:	November 2020
EDRMS File Reference:	D19/440697/DJ
Key Words:	Guidance, protocol, assessment, privacy codes, PPIP Act, HRIP Act

Version	Date	Reason for amendment
1.1	June 2014	Review
1.2	December 2014	Accessibility update
1.3	November 2019	Updated