

protocol

Protocol on
Assessing Draft Privacy Codes of Practice
under the PPIP Act and HRIP Act



privacy**ns**w

Issue date: 13 May 2004

Privacy NSW Protocol

Assessing Draft Privacy Codes of Practice under the PPIP Act and HRIP Act

What is a privacy code of practice?

Under the PPIP Act

Under the Privacy and Personal Information Protection Act 1998 (the PPIP Act), NSW public sector agencies are bound to comply with:

- the information protection principles (IPPs), and
- the public register provisions in Part 6 of the PPIP Act.

A Privacy Code of Practice may be made under the PPIP Act to modify the application of the IPPs or the public register provisions of the Act, or specify how they are to be applied to particular activities or classes of information. A Code may affect one or more public sector agencies.

Under the HRIP Act

Under the Health Records & Information Privacy Act 2002 (HRIP Act), NSW public sector agencies are bound to comply with:

- the health privacy principles (HPPs).

Also under the HRIP Act, private sector individuals and organisations are bound to comply with:

- the health privacy principles (HPPs), and
- the special rules on keeping and providing access and amendment to health information in Part 4 of the HRIP Act.

A Health Privacy Code of Practice may be made under the HRIP Act to modify the application of the HPPs or the provisions of Part 4 of the Act, or specify how they are to be applied to particular activities or classes of information. A Code may affect one or more public sector agencies and/or private sector persons and organisations.

Why might a privacy code of practice be needed?

A Privacy Code of Practice might sometimes be needed where, in the operations of an organisation, privacy has to be balanced against other public interests. Codes of practice must still meet a number of requirements to ensure that they protect privacy.

How is a privacy code of practice made?

Codes are drafted by Parliamentary Counsel, and published in the Government Gazette. In order to be made, codes must first be approved by the relevant Minister, after certain steps have been followed.

- For codes under the PPIP Act, the relevant Minister is the Attorney General, who must consult with the Privacy Commissioner.
- For codes under the HRIP Act, the relevant Minister is the Minister for Health, who must consult with both the Attorney General and the Privacy Commissioner.

Prior to a draft code being sent to the relevant Minister for approval, draft codes must be sent to the Privacy Commissioner for review. The Privacy Commissioner may make a submission to the organisation proposing the draft code, and ultimately to the Attorney General and/or the Minister for Health.

Organisations wishing to prepare a draft code should therefore give Privacy NSW advance notice so that we can make suggestions on the need for a code and any supporting case. We strongly suggest that agencies submit a separate business case before preparing their draft code to explain why a code is needed. This allows the justification for making a code to be assessed before any unnecessary work is spent on a draft code which may ultimately be assessed as not necessary or justified.

Once the general proposal has been agreed to, only then will Parliamentary Counsel be instructed to prepare a draft code for further review and consultation.

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

The Privacy Commissioner has the responsibility of making recommendations to the Attorney General 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. 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.

These two Acts confers privacy rights on and recognise expectations of individuals in a way which furthers the aims of international conventions to which Australia is a party. In assessing and making recommendations, the Privacy Commissioner has a responsibility to give effect to the intention of the two Acts, and minimise the potential of codes to lessen these rights and expectations.

The validity of a privacy code of practice depends on a number of conditions specified in the two Acts. 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.

In reviewing draft privacy codes of practice and making submissions to the Attorney General and/or Minister for Health as to whether or not to approve a draft code, the Privacy Commissioner will have regard to the following matters.

1 Scope

1.1 Does the proposed code:

Under the PPIP Act:

- modify the application of any one or more of the IPPs to any public sector agency?
- modify the application of Part 6 of the PPIP Act to any public sector agency?
- 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?
- exempt a public sector agency, or class of public sector agencies, from the requirement to comply with any IPP?

- clearly indicate the extent of any such modification, specification or exemption?

Under the HRIP Act:

- modify the application of any one or more of the HPPs to any public or private sector person or organisation?
- modify the application of the provisions of Part 4 of the HRIP Act to any private sector person or organisation?
- 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?
- 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?
- clearly indicate the extent of any such modification, specification or exemption?

2 Coverage

2.1 Does the proposed 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, or
- the activity or class of activities

in relation to which the code purports to modify the IPPs or HPPs?

2.2 Is the class of information, organisations or activities more widely defined than is necessary to achieve the intention of the proposed code or code provision?

3 Consistency : Is the proposed code consistent with the stated purpose of the relevant Act?

3.1 Is it made for the purpose of protecting the privacy of individuals?

3.2 Do the IPPs or HPPs, as modified by each of the provisions of the proposed code, on balance still protect privacy?

As a general principle the privacy interests of individuals are best secured through consistent adherence to the principles by all organisations. A multiplicity of exceptions will make it difficult for individuals to have consistent expectations and to exercise their rights under the two Acts.

In assessing how a proposed modification of a principle affects privacy, the principles should be viewed as each contributing to an overall result rather than operating in isolation. For example, removing the requirement to collect information directly from the individual under IPP 2 or HPP 3 might not affect the individual's privacy as long as the individual was notified of the collection under IPP 3 or HPP 4. However, because IPP 3 applies only to information collected from an individual, such a trade-off would need to be carefully worded to avoid imposing a higher standard on the agency.

3.3 Does the proposed 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?

Privacy legislation passed or proposed in other jurisdictions (most notably the European Union) requires that external transfers of personal information should only be made where there is an adequate or comparable level of protection in the receiving jurisdiction.

The European Union's Data Protection Working Party carried out an assessment of the Federal Privacy Act in 2001 and concluded that data transfers to Australia could be regarded as adequate only if appropriate safeguards were introduced to meet a range of concerns over adequacy. The Working Party went on to recommend voluntary codes of conduct enforced by the Federal Privacy Commissioner or by an independent adjudicator.

The Working Party did not consider the relevance of the PPIP Act to disclosures to NSW public sector agencies and it is doubtful whether or how their reservations would apply to such disclosures. In these circumstances the Privacy Commissioner takes a relatively flexible approach to section 29(7)(a) of the PPIP Act and section 38(6)(a) of the HRIP Act, taking into account:

- whether the organisation(s) proposing the code customarily shares personal information with other jurisdictions; and
- any privacy legislation in jurisdictions which share data with the organisation(s) proposing the code.

Where a provision of a proposed code authorises the sharing of personal information with organisations in another jurisdiction, other matters to be considered will include:

- policies on privacy protection for the recipient organisations in the other jurisdiction
- any relevant privacy protection or complaint investigation bodies in the other jurisdiction
- whether the proposed disclosure is to a public sector or private sector body
- the ability to enforce contractual undertakings which the New South Wales organisation may impose on a transfer
- the public interest in giving effect to proposed transfers (for example in the sharing of information between revenue agencies to minimise avoidance or the sharing of information between law enforcement agencies)
- whether proposed transfers would be more appropriately covered by a separate code of practice (for example under section 19(4) of the PPIP Act)

3.4 Does the proposed code impose on any organisation requirements that are more stringent (or of a higher standard) than the IPPs or HPPs?

Codes or code provisions which impose higher or more stringent standards than the relevant set of principles risk invalidity under section 29(7)(b) of the PPIP Act or section 38(6)(b) of the HRIP Act. This does not prevent an organisation from imposing more stringent conditions on itself or on its contractors. Nor does it prevent an organisation which is bound by other obligations in relation to personal information or health information (e.g. legal obligations of confidentiality or statutory confidentiality provisions) from prescribing higher standards in an applicable document which is not a privacy code of practice within the meaning of the two Acts.

3.5 Do any provisions of the proposed code purport to modify an applicable exemption?

Under section 29(6) of the PPIP Act and section 38(5) of the HRIP Act, such a provision in a code is invalid. Organisations submitting proposed codes which include departures from the principles which are already covered by another exemption will be encouraged to remove them.

3.6 Does the proposed code substantially affect privacy or other interests of an identifiable group of people, if so:

- is the code discriminatory?
- has there been appropriate consultation?

In some circumstances the Privacy Commissioner may recommend that a code proceed subject to a sunset clause to allow fuller consultation before a final code is made.

3.7 Will the proposed 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 code.

3.8 Are the alterations to the IPPs or HPPs clearly expressed and readily understandable?

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.

3.9 Has the organisation provided a business case that justifies the making of a code?

3.10 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.

4 Public register provisions

In assessing a proposed code which seeks to modify the public register provisions in the PPIP Act, the following issues will be considered in addition to those matters already covered in this protocol:

- the purpose of the register or the legislation setting up the register
- the nature of the information contained on the register
- the steps proposed to be taken by the agency to establish the purpose for which access to the register is being given
- other matters which may render compliance with the public register provisions unreasonable or onerous, including:
 - the public interest in maintaining relatively unrestricted access to a given register
 - the form in which public access is given to the register (for example access to a folio or screen or the issue of a certificate)
 - the means of establishing reasons for accessing a particular register; and whether the steps reasonably necessary for an agency to satisfy itself that the proposed use of personal information are consistent with the purpose of the register or would unreasonably restrict public access to the register
 - whether proposed uses would or would not otherwise unreasonably interfere with personal privacy

- the difficulty of complying with the test in section 58(2) when dealing with an application to suppress information
- the practical difficulty in excluding information subject to an application for suppression, having regard to the manner in which the register is made available to the public
- the practicality of giving individuals the option to consent to their personal information being made available from the register
- the possibility of meeting the public register provisions in part but modifying them in relation to more limited classes of sensitive information on a register.

5 Overall effect

5.1 Impact on accountability mechanisms

Will the proposed code unduly impact on the ability of an aggrieved person to seek review of an organisation's conduct in the Administrative Decisions Tribunal?

A matter may proceed to the Administrative Decisions Tribunal 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.

As a general proposition an exemption drafted as part of a code should not be worded so broadly that it prevents the Administrative Decisions Tribunal reviewing conduct of the organisation that may contravene the overall intention of, or breach the spirit of, the relevant privacy principles. Consequently provisions which permit a departure where reasonably necessary to fulfil a legitimate function of an organisation will be preferred to provisions which gives an absolute exemption, or provisions the exercise of which are wholly dependant on the discretion of the organisation itself.

5.2 Is the making of the proposed code in the public interest?

Overall, do the benefits of making a particular code outweigh the public interest in having a consistent and standardised privacy regime?