

Privacy Internal Review Guidelines NSW Health

Document Number GL2006_007

Publication date 24-May-2006

Functional Sub group Corporate Administration - Records
Clinical/ Patient Services - Records
Personnel/Workforce - Conditions of employment
Personnel/Workforce - Conduct and ethics

Summary This Guideline provides guidance for NSW Health staff on the handling of privacy complaints and the process of internal review in relation to the Privacy and Personal Information Protection Act 1998 and the Health Records and Information Protection Act 2002.

Author Branch Legal and Legislative Services

Branch contact Victoria Monahan 9391 9092

Applies to Area Health Services/Chief Executive Governed Statutory Health Corporation, Board Governed Statutory Health Corporations, Affiliated Health Organisations, Public Health System Support Division, Community Health Centres, Dental Schools and Clinics, NSW Ambulance Service, NSW Dept of Health, Public Health Units, Public Hospitals

Audience All staff

Distributed to Public Health System, Community Health Centres, Dental Schools and Clinics, Health Associations Unions, Health Professional Associations and Related Organisations, NSW Ambulance Service, NSW Department of Health, Public Health Units, Public Hospitals, Tertiary Education Institutes

Review date 24-May-2011

File No. 04/2799-02

Status Active

NSW Health Privacy Internal Review Guidelines



NSW DEPARTMENT OF HEALTH

73 Miller Street
NORTH SYDNEY NSW 2060
Tel. (02) 9391 9000
Fax. (02) 9391 9101
TTY. (02) 9391 9900

www.health.nsw.gov.au

This work is copyright. It may be reproduced in whole or in part for study training purposes subject to the inclusion of an acknowledgement of the source. It may not be reproduced for commercial usage or sale. Reproduction for purposes other than those indicated above, requires written permission from the NSW Department of Health.

© NSW Department of Health 2006

SHPN (LLSB) 060077
ISBN 0 7347 3951 6

For further copies of this document please contact:

Better Health Centre – Publications Warehouse
Locked Mail Bag 5003
Gladesville NSW 2111
Tel. (02) 9816 0452
Fax. (02) 9816 0492

Further copies of ***NSW Health Privacy Internal Review Guidelines***

documents can be downloaded from the:

NSW Health website: www.health.nsw.gov.au/privacy

Intranet: internal.health.nsw.gov.au/publications

May 2006

Contents

Introduction	2	Appendix 1. Information sheet for Privacy Internal Review	10
1. Background	3	Appendix 2. Privacy complaint: Internal Review Application Form	11
1.1 When do these Guidelines apply?	3	Appendix 3. Letter of receipt to applicant	13
1.2 Overview of Guidelines	3	Appendix 4. Letter of notification to Privacy Commissioner	14
1.3 Complaints handling and the process of internal review	4	Appendix 5. Letter of preliminary findings to Privacy Commissioner	15
2. Internal Review Process	5	Appendix 6.1. Internal review letter and report pro formas	16
2.1 Information about internal review processes	5	Appendix 6.2. Report of internal review	17
2.2 Privacy Contact Officer	5	Appendix 7. Checklist for internal review	20
2.3 The application for internal review	5		
2.3.1 The application form	6		
2.4 The Review Officer	6		
2.5 Receipt of application for internal review	6		
2.6 The internal review	6		
2.6.1 The conduct of the review	6		
2.6.2 Completion of the internal review	7		
2.6.3 Notification of the applicant	7		
2.6.4 Annual reporting requirements	7		
3. The role of the Privacy Commissioner	8		
3.1 Monitoring progress	8		
3.2 Complaints relating to privacy	8		
4. References	9		

Introduction

Privacy laws govern all aspects relating to the management of personal information held by an agency in NSW. *The Health Records and Information Privacy Act (HRIP) Act 2002* governs personal health information and the *Privacy and Personal Information Protection (PPIP) Act 1998* governs all other personal information.

The provisions for internal review for both Acts are set out in Part 5 of the PPIP Act. These provisions should be used irrespective of whether the alleged breach arises under the HRIP Act or the PPIP Act.

The Internal Review provisions allow individuals to seek a review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the privacy laws.

Internal Reviews are to be undertaken in accordance with these guidelines which reflect the provisions of the PPIP Act and are based on guidelines issued by Privacy NSW.

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

- breached any of the Health Privacy Principles that apply to the agency under the HRIP Act (for further details, **see NSW Health Privacy Manual**), or

- breached any of the Information Protection Principles that apply to the agency under the PPIP Act (for further details, **see NSW Health Privacy Management Plan**, Part 1),
- breached any code or direction made under either Acts applying to the agency, or
- disclosed information on a public register except in accordance with Section 57 (PPIP Act only)

Important note

All privacy complaints, enquiries about privacy, and requests for internal review, should be treated as serious matters. Individuals who have made an application for internal review may apply to the Administrative Decisions Tribunal (ADT) if they are not satisfied with either the findings of the internal review, or the action taken by the agency in relation to their application for review. The ADT can make orders, including the imposition of fines up to \$40,000.

1.1 When do these Guidelines apply?

Where a person requests an internal review, there are certain legislative requirements regarding how and when the application can be made, and how it should be dealt with. This document is designed to provide detailed guidelines to NSW Health agencies in respect of these obligations.

Where a person raises general concerns as to how personal or personal health information is being handled and does not indicate that they are personally aggrieved by the conduct, agencies should seek to address the person's concerns by reference to the agency's existing information management policies and guidelines for complaints handling. For example, a patient may express concern about the number of staff accessing their medical record. The patient may not seek a privacy internal review of this practice, rather some explanation and reassurance regarding staff duties of confidentiality. Another example may be where a member of the public has overheard a staff member discussing a patient socially. The person may wish to bring the incident to the attention of hospital management, rather than to request a privacy internal review.

Where the person's concerns cannot be resolved through existing policies and guidelines, an agency must provide the person with information relating to their rights to an internal review under privacy laws, and the requirements for lodging an application for review. If the person chooses to exercise these rights, the terms of these guidelines will apply.

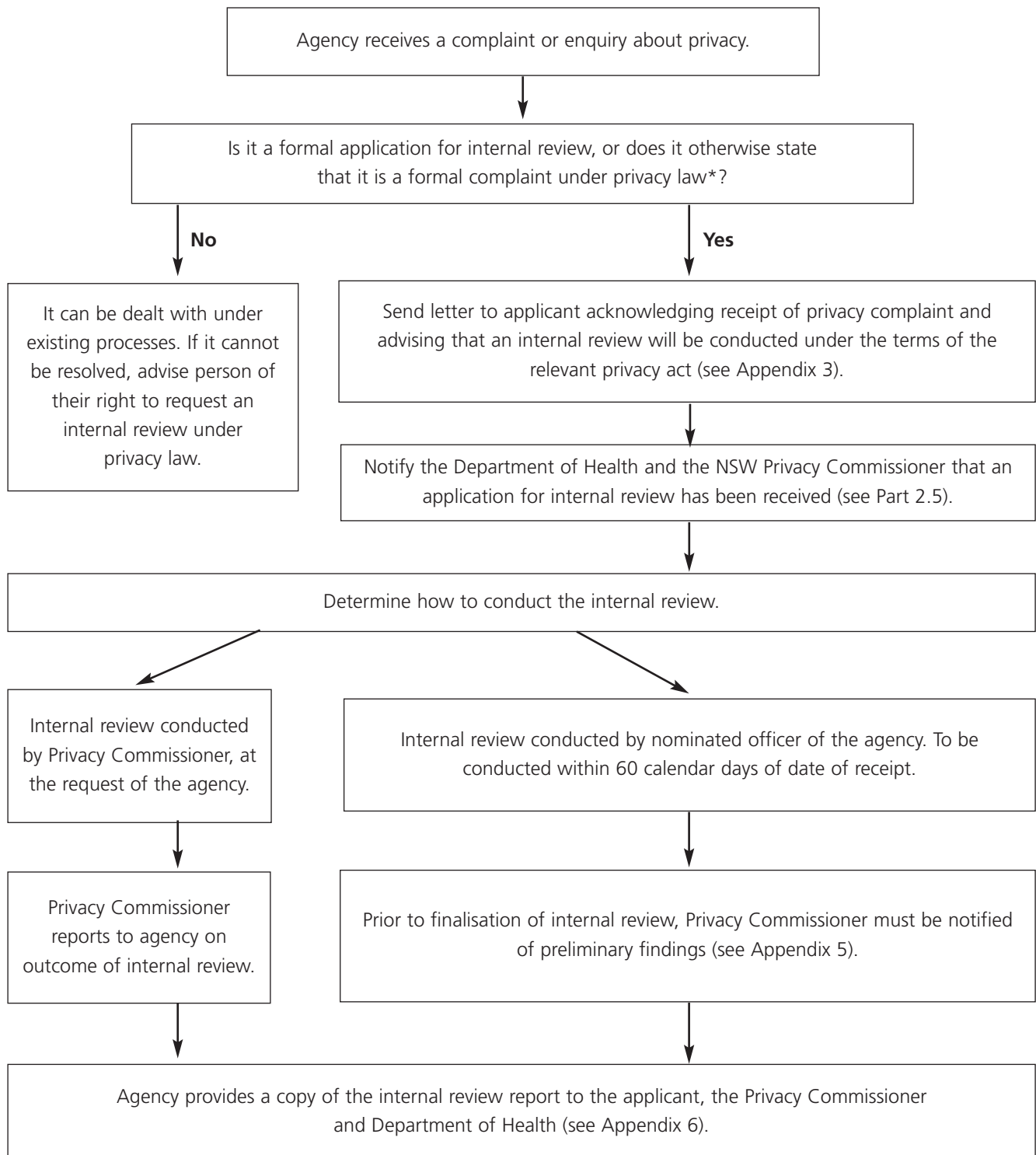
1.2 Overview of Guidelines

These guidelines set out how agencies are to fulfill their internal review obligations. To this end, they provide information, including:

- how agencies can ensure information about complaint and internal review rights is available to individuals
- application forms and pro forma letters and reports which can be used in internal reviews
- guidance on who will process applications, and how this will be done, including the time frames for completion of the internal review
- information on the role of the Privacy Commissioner in the internal review process
- explanation of agencies' obligations to notify the Commissioner at different stages of the internal review.

1.3 Complaints handling and the process of internal review

The flow chart below describes the process for handling a privacy complaint, and serves as a quick reference summary of the guidelines set out in these guidelines.



*A complaint under privacy law can relate to either the Privacy and Personal Information Protection Act 1998 or the Health Records and Information Privacy Act 2002. Complaints under both Acts are dealt with in Part 5 of the Privacy and Personal Information Protection Act 1998.

2.1 Information about internal review processes

As part of fulfilling its obligations under privacy law, agencies must ensure information is available to inform individuals of their right to request an internal review, and of their right to seek a review by the ADT.

Requests for information relating to internal review or to answer questions relating to internal review are to be directed to the agency's Privacy Contact Officer.

A pro forma Information Sheet for this purpose, which includes information about the requirements for requesting an internal review, is set out in Appendix 1. This Information Sheet is to be adapted by the agency to include its name and contact details and must be provided to individuals requesting information about the privacy internal review process.

The NSW Health Privacy Leaflet For Patients also provides contact details for individuals if they have a privacy complaint (see NSW Health Privacy Manual, Appendix 5). Both the Information Sheet and Privacy Leaflet For Patients should be sent to internal review applicants with the letter acknowledging receipt of their application (see Section 2.5).

2.2 Privacy Contact Officer

The Department of Health, the Ambulance Service of NSW, Area Health Services, affiliated health organisations and statutory health organisations are required to nominate a person to act as Privacy Contact Officer for that agency.

Contact details for NSW Health Privacy Contact Officers are available on the NSW Health Internet and Intranet privacy pages (see Section 4).

The Privacy Contact Officer is responsible for ensuring the agency meets its obligations under the Act, including keeping the Privacy Commissioner informed of the progress of internal reviews, and of the action proposed to be taken by the agency in relation to the matter. These notifications must be in writing.

The Privacy Contact Officer must also keep statistical details about the number of internal review requests received. These statistics will be included in the agency's annual report, in compliance with section 33(3) of the Act.

The Chief Executive may request that the Privacy Contact Officer conducts the internal review, as long as this officer was not substantially involved in any matter relating to the conduct which is the subject of the application. If this is the case, the Chief Executive must request that an alternative Review Officer conducts the internal review (see Section 2.4).

2.3 The application for internal review

Application for internal review can only be submitted by a person who is "aggrieved" by the conduct of the agency in relation to their information privacy. In particular, the individual may believe that the agency has breached any of the Information Privacy Principles under the PPIP Act, or the Health Privacy Principles under the HRIP Act.

It is important to recognise that a "person aggrieved" 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. Sometimes a third party can also be affected by a disclosure. Where the applicant is not the individual to whom the information relates, the agency should assess the application to identify if this person has been directly affected by the alleged breach.

An application for internal review must, under section 53 (3) of the PPIP Act:

- be in writing
- be addressed to the agency
- 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 six months (or such later date as the agency may allow) from the time the applicant first became aware of the conduct sought to be reviewed.

2.3.1 The application form

An application form to assist individuals apply for an internal review has been developed for NSW Health based on the application form provided by NSW Privacy Commission (see Appendix 2).

This form should be forwarded to prospective applicants where possible. The form allows the applicant to state which privacy principles they believe have been breached, and what action they would like the agency to take as a result, which can facilitate clear communication between the individual and the agency. While the form is therefore useful to both applicant and the agency, an applicant is not obliged to use it. As long as the application is received in writing, the agency must process it as an internal review application.

2.4 The Review Officer

An application for internal review must be dealt with by an individual within the agency who must be, as far as is practicable, a person who:

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

A person may be considered substantially involved in a matter where they have 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.

In most cases, the Review Officer will be the agency's Privacy Contact Officer (see Section 2.2), unless this person was substantially involved in the matter relating to the complaint.

2.5 Receipt of application for internal review

When an internal review application is received by an agency, it is to be forwarded to the agency's Privacy Contact Officer for review or to another suitable Review Officer.

As soon as practicable after receiving the application, the Review Officer is required to:

- write to the applicant to acknowledge receipt of

their application, and to advise that their application will be reviewed within 60 calendar days, and that the Privacy Commissioner will be kept informed of the progress of the internal review, as required by the PPIP Act (see Appendix 3 for pro forma Letter of Receipt to Applicant), and

- write to the Privacy Commissioner to advise that an application for internal review has been received, and to provide a copy of the application (where the applicant has consented, or not objected) (see Appendix 4 for pro forma Letter of Notification to Privacy Commissioner), and
- notify the Privacy Contact Officer, Department of Health of the application by telephone (Tel. 02 9391 9605) or e-mail (privacy@doh.health.nsw.gov.au).

2.6 The internal review

2.6.1 The conduct of the review

In the initial stages of the review, the Reviewing Officer must consider any relevant material submitted by the applicant, and by the Privacy Commissioner.

The Review Officer must gather further information relating to the events and conduct which led to the complaint. Depending on the nature of the issues raised, and the circumstances in which the alleged breach arose, this might include:

- seeking further information from the applicant. The Review Officer should seek clarification or additional information from the applicant as necessary
- reviewing internal documents or other relevant documentation, including for example the applicant's medical file or other material held by the agency which is relevant to the application
- interviewing staff who were involved in dealing with the matter which is the subject of the application

All gathering of information must be fully documented, kept confidential and be used only for the purpose of the review, or in accordance with NSW Health Privacy Manual.

In light of the information gathered, the Review Officer must then consider whether the agency's conduct has breached any of the Information Privacy Principles under the PPIP Act, or Health Privacy Principles under the HRIP Act, or (where relevant) a code or a public register provision under either Act.

Prior to finalisation of the Internal Review Report, the agency must inform the Privacy Commissioner of the preliminary findings of the review and as far as practicable provide sufficient time for the Privacy Commissioner to comment on these findings, which can be negotiated in advance. See Appendix 5 for a pro forma Letter of Preliminary Findings to Privacy Commissioner.

For further assistance, refer to the 'Internal Review Checklist for the Respondent Agency' issued by Privacy NSW (see Section 4).

2.6.2 Completion of the internal review

The process of internal review, and the outcome as to whether the agency considers that a breach has or has not occurred, must be documented in an Internal Review Report. Any comments with regards to the review received from the Privacy Commissioner should be taken into consideration when preparing the final report.

See Appendix 6 for a pro forma Internal Review Report to assist in the writing of the report.

The report must recommend any one or more of the following in response to the review:

- take no further action on the matter
- make a formal apology to the applicant
- take such remedial action as it thinks appropriate (for example, the payment of monetary compensation to the applicant)
- 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, and privacy training for relevant staff.

Important note

The Reviewing Officer must complete the review as soon as is reasonably practicable within the circumstances, and in any event, within 60 calendar days from the day on which the application was received by the agency. If the review is not completed within 60 calendar days, the applicant is entitled to make an application to the Administrative Decisions Tribunal for a review of the conduct concerned.

2.6.3 Notification of the applicant

Within 14 calendar days after the completion of the review, the Privacy Contact Officer must notify the applicant in writing of:

- the findings of the review (and the reasons for those findings), and
- the action proposed to be taken by the agency (and the reasons for taking that action), and
- the right of the person to have those findings and the agency's proposed action reviewed by the Administrative Decisions Tribunal.

Where the agency has taken the full 60 calendar days to conduct the internal review, the report must be sent to the applicant as soon as possible, and the applicant should be contacted to advise when they can expect to receive the report.

A copy of the final report must also be sent to the Department of Health (see Appendix 6.1).

To assist the Reviewing Officer with the internal review process, see Appendix 7 for a Checklist for Internal Review to ensure all statutory requirements are met.

2.6.4 Annual reporting requirements

The annual report of each agency must include:

- a statement of the action taken by the agency in complying with the requirements of this Act, such as the delivery of privacy training to staff, the distribution of information regarding privacy to patients, and so on.
- statistical details of any internal review(s) conducted by (or on behalf of) the agency as directed by this document, including when the application for each review was received, and a summary of the outcome of the review. The summary should include whether it was found that any privacy principles were breached, and the broad context of the breach. If the applicant sought further review in the Administrative Decisions Tribunal, a summary of these findings should also be provided.

Care must be taken to ensure that the details included in the annual report can in no way identify an applicant of internal review.

3.1 Monitoring progress

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

- notify the Privacy Commissioner of the application as soon as practicable (see Appendix 4), and
- keep the Privacy Commissioner informed of the progress of the internal review, and
- inform the Privacy Commissioner of the preliminary findings of the review and of the action proposed to be taken by the agency in relation to the matter (see Appendix 5).

3.2 Complaints relating to privacy

The Privacy Commissioner can also receive and investigate complaints directly from individuals who are concerned about the alleged violation of, or interference with, the privacy of an individual's personal or personal health information. This option for a person exists quite separately from the right to an internal review, and can cover the same conduct.

A complaint may be in writing or verbal, but the Privacy Commissioner may require a verbal complaint to be put in writing. The Privacy Commissioner may require information about a complaint to be provided by the complainant in a particular manner, and may require a complaint to be verified by statutory declaration.

A complaint must be made within six months (or such later time as the Privacy Commissioner may allow) from the time the complainant first became aware of the conduct or matter that was the subject of the complaint. A complainant may amend or withdraw a complaint.

NSW Health publications

NSW Health Privacy Manual, PD2005_593

NSW Health Privacy Management Plan, PD2005_554

NSW Health Privacy Intranet page:

<http://internal.health.nsw.gov.au/privacy>

NSW Health Privacy Internet page:

<http://www.health.nsw.gov.au/privacy>

NSW Health Privacy Leaflet for Patients:

<http://www.health.nsw.gov.au/privacy/leaflets.html>

Privacy NSW publications

Privacy NSW Internet page:

<http://www.lawlink.nsw.gov.au/lawlink/privacynsw>

Privacy NSW 'Internal Review Checklist for the Respondent Agency':

http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_publications

Appendix 1

Information sheet for Privacy Internal Review

Internal review is a process whereby this agency will handle complaints about how it has dealt with personal information under the *Privacy and Personal Information Protection (PPIP) Act 1998* and/or personal health information under the *Health Records and Information Privacy (HRIP) Act 2002*.

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

The request for review can only be made where it is alleged that the agency 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 agency
- breached any code made under the Acts applying to the agency
- disclosed personal or personal health information kept in a public register.

The request for internal review should be lodged using an application form available from NSW Health or the NSW Privacy Commission. This application should be sent direct to the agency within six months from the time the applicant first became aware of the conduct sought to be reviewed, or at an earlier date as decided by the agency if special circumstances apply.

The Privacy Commissioner will be notified of the application, the progress and findings of the internal review to allow for submissions to be made to the agency where appropriate. The Privacy Commissioner will subsequently be notified of the action proposed to be taken by the agency in relation to the matter.

A Review Officer will be appointed to conduct the internal review, which will be completed within 60 calendar days from the day on which the application is received. If the review is not completed within 60

calendar days, the applicant is entitled to make an application to the Administrative Decisions Tribunal for a review of the conduct concerned. In order to investigate the circumstances surrounding the complaint, the Review Officer may need to discuss the matter with relevant staff members and seek legal advice from the Department of Health. All information held by the agency in connection with the complaint will otherwise be kept secure and held in confidence.

The review must recommend that the agency respond in any one or more of the following ways:

- take no further action on the matter
- make a formal apology to the applicant
- take such remedial action as it thinks appropriate
- 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, and privacy training for relevant staff.

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

- the findings of the review and the reasons for those findings, and
- the action proposed to be taken by the agency including the reasons for taking that action, and
- the right of the person to have the agency's findings and proposed action reviewed by the Administrative Decisions Tribunal.

If an applicant is not satisfied with the findings of the review, or the action taken by the agency in relation to the application, the applicant may apply to the Administrative Decisions Tribunal for a review of the conduct that was the subject of the application for internal review.

[Include name and contact details of Privacy Contact Officer for relevant agency (see NSW Health Privacy Internet Page for details)].

Appendix 2

Privacy Complaint: Internal Review Application Form

This is an application¹ for review of conduct under:

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

(please choose one – see www.lawlink.nsw.gov.au/privacynsw for further information on the two Acts)

1. Name of the agency ² you are complaining about:
2. Your full name:
3. Your postal address:
4. If you are complaining on behalf of someone else, write their full name here: What is your relationship to this other person (eg parent)? Is the other person capable of making the complaint him or herself? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> I'm not sure
5. What is the specific conduct ³ you are complaining about?
6. Please tick which of the following describes your complaint: (<i>You can tick more than one</i>) <input type="checkbox"/> collection of my personal/health information <input type="checkbox"/> security or storage of my personal/health information <input type="checkbox"/> refusal to let me access or find out about my own personal/health information <input type="checkbox"/> accuracy of my personal/health information <input type="checkbox"/> use of my personal/health information <input type="checkbox"/> disclosure of my personal/health information <input type="checkbox"/> other <input type="checkbox"/> I'm not sure

Appendix 2

7. When did the conduct occur? <i>(Please be as specific as you can)</i>
8. When did you first become aware of this conduct?
9. You need to lodge this application within 6 months of the date you have written at Q.8. <i>If more than 6 months has passed, you need to ask the agency for special permission to lodge a late application. If you need to, write here to explain why you have taken more than 6 months to make your complaint:</i>
10. What effect did the conduct have on you?
11. What effect might the conduct have on you in the future?
12. What would you like to see the agency do about the conduct? <i>(For example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)</i>
13. <input type="checkbox"/> I understand that this form will be used by the agency to process my request for an Internal Review. <input type="checkbox"/> I understand that details of my application will be referred to the Privacy Commissioner in accordance with: section 54 (1) of the <i>Privacy and Personal Information Protection Act 1998</i> ; or section 21 of the <i>Health Records and Information Privacy Act 2002</i> ; and that the Privacy Commissioner will be kept advised of the progress of the Review.
14. I would prefer the Privacy Commissioner to have: <input type="checkbox"/> a copy of this application form, or <input type="checkbox"/> just the information provided at Q's 5–12.

Your signature:

Dated:

NOW SEND THIS FORM TO THE AGENCY YOU HAVE NAMED AT Q.1

Keep a copy for your own records too.

- 1 This application form has been adopted with permission from Privacy NSW. It is not a requirement under the PPIP Act/the HRIP Act that you complete an application form. This form is designed for your convenience only.
- 2 The PPIP Act regulates NSW State government departments, Area Health Services, most other State government bodies, and NSW local councils. Each of these is defined as a "public sector agency". The HRIP Act regulates private and public sector agencies and private sector persons.
- 3 'Conduct' can include an action, a decision, or even inaction by the agency. For example the 'conduct' in your case might be a *decision* to refuse you access to your personal information, or the *action* of disclosing your personal information to another person, or the *inaction* of a failure to protect your personal information from being inappropriately accessed by someone else.

Appendix 3

Letter of receipt to applicant

Date

Applicant's name

Applicant's address

Dear [Applicant's name]

RE: Application for Internal Review

I wish to acknowledge receipt of your application for an Internal Review by [name of health service] on the [date].

Your application will be reviewed having regard to the requirements of the Health Records and Information Privacy Act 2002 (if health information) OR the Privacy and Personal Information Protection Act 1998, (if personal information).

Under the law, [name of health service] is allowed 60 calendar days to conduct the Internal Review from the day on which the application was received, which is [date of completion]. We will contact you if for any reason the Internal Review has not been finalised by this date. Alternatively, you may request that an external review be carried out by the Administrative Decisions Tribunal.

In my role as [eg Privacy Contact Officer], and being independent of the circumstances surrounding your complaint, I have been asked to oversee this review on behalf of the Chief Executive.

The law requires that the NSW Privacy Commissioner be notified of this application and be advised of the progress of the review, and a copy of your application has been forwarded to the Office of the Privacy Commissioner [*if applicant has consented, or not objected*].

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

Yours sincerely

(eg Privacy Contact Officer/or Review Officer)

Enclosed: – Information Sheet for Privacy Internal Review [see Appendix 1]
– Privacy Leaflet for Patients [see NSW Health Privacy Manual]

Appendix 4

Letter of notification to Privacy Commissioner

Date

Mr John Dickie
A/Privacy Commissioner
GPO Box 6
Sydney NSW 2001

Dear Mr Dickie

RE: Application for Internal Review by [name of applicant]

This is to advise that an application for an Internal Review was received by [name of health service] 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 an agency 60 calendar days to conduct the Internal Review from the day on which the application was received, the AHS must complete the review by [date].

A copy of the application is attached for your reference. *[Note: only include this where the applicant has consented or has not objected.]*

I recognise that under section 54(2) of the Act, your office is 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].

Yours sincerely

Privacy Contact Officer or Review Officer

Appendix 5

Letter of preliminary findings to Privacy Commissioner

Date

Mr John Dickie
A/Privacy Commissioner
GPO Box 6
Sydney NSW 2001

Dear Mr Dickie

RE: Notice of Preliminary Findings

Please find attached the preliminary findings for the application for internal review received by us from [name of applicant].

Your office was previously notified of the details of this review in our letter, dated [date]. Under the terms of the Privacy and Personal Information Protection Act, the review must be completed by the AHS 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.

(Insert a brief description of nature of complaint.)

Preliminary findings

[State whether, in the preliminary view of the health service, a privacy breach has or has not occurred.]

[State which actions the agency is considering taking as a result of the findings, for example:

- take no further action*
- make a formal apology to the applicant*
- take remedial action (including for example, amendment of records, revised model of care for client, compensation, etc)*
- provide undertakings that the conduct will not occur again*
- implement administrative measures to ensure that the conduct will not occur again*

[Reference: Privacy and Personal Information Protection Act 1998, section 53 (7).]

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

Yours sincerely

Privacy Contact Officer, or Review Officer

cc: Privacy Contact Officer, Legal and Legislative Services Branch, NSW Department of Health

Appendix 6.1

Internal review letter and report pro formas

Date

Name of applicant

Our ref.

Address

Dear [Applicant's name]

I write to you in reference to your complaint dated [date] addressed to the [*name of officer and health service who have received the complaint*] regarding [*summarise briefly 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 health 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.

If you are dissatisfied with the outcome of this review, the Act provides you with a right to lodge an appeal to the Administrative Decisions Tribunal within 28 calendar days from receipt of this correspondence (+ 5 calendar days for postage). The contact details for this agency are listed as follows:

Administrative Decisions Tribunal
Level 15, 111 Elizabeth Street
SYDNEY NSW 2000
Telephone: 9223 4677
Facsimile: 9233 3283

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 of Review Officer, health service] on [telephone number].

Yours sincerely,

Privacy Contact Officer, or Review Officer

cc: Privacy Contact Officer, Legal and Legislative Services Branch, NSW Department of Health

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

Appendix 6.2

Report of internal review under the PPIP Act 1998/HRIP Act 2002 [delete as appropriate]

1. Background

This internal review arises out of an application by [insert name of applicant]. The application relates to events that took place at [describe location] on [describe time frame].

** Variable content: 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. 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.*

2. Application for internal review

** Variable content: Summarise:*

- when application was received*
- when letter of receipt was sent to the applicant*
- when Privacy Commissioner was advised*
- when internal review was commenced*

and any other relevant chronology.

3. Internal review

(Standard Text)

Two pieces of Privacy Legislation operate in NSW. The Health Records and Information Privacy Act (HRIP Act) regulates “health information” through 15 Health Privacy Principles (or HPPs). The Privacy and Personal Information Protection Act (PPIP Act) regulates general personal information (other than health information) through 10 Information Protection Principles and also regulates the review of conduct by public sector agencies for both Acts.

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.

3.1 Is the information in question “personal information” and/or “health 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”

Appendix 6.2

* Determine whether the application relates to “personal information”, and indicate briefly why.

Section 6 of the HRIP Act defines “health 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 health services to him or her, or*
 - (iii) *a health service provided, or to be provided, to an individual, or*
- (b) *other personal information collected to provide, or in providing, a health service, or*

* Determine if the application relates to “personal health information”, and indicate briefly why.

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

3.2 Is the AHS the appropriate agency to deal with the complaint?

* *Ensure you have identified that your AHS is the appropriate agency to deal with the matter, and indicate why.*

3.3 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 a “person aggrieved”.*

3.4 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.*

4. Alleged breaches of the PPIP ACT 1998/HRIP ACT 2002

 [delete as appropriate]

* *List and summarise each of the Information Privacy Principles/or Health Privacy Principles identified as relevant, and identify whether the agency’s conduct has breached each Principle, for example:*

4.1 Terms of Information Privacy Principle X/or Health Privacy Principle X

* *Insert actual wording of Principle.*

4.2 Conduct/Assessment

* *Summarise outcome of review, refer to documents considered and identify whether the conduct in question has/has not breached the relevant Principle.*

Conclude with:

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

[Repeat for each Principle identified at 4.1.]

5. Findings

* *Summarise findings, for example:*

The findings of this internal review conclude that there has/has not been a breach of the Information Privacy 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).*

6. Recommendations

(Standard Text)

Section 53(7) of the Privacy and Personal Information Protection Act sets out a range of options which can be recommended at the end of the internal review. These are to:

- take no further action on the matter
- make a formal apology to the applicant
- take such remedial action as it thinks appropriate (for example, the payment of monetary compensation 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).

In this case, the applicant has sought: *(identify what the applicant has asked to occur – irrespective of whether these fall within the above categories).*

** Set out the recommendations (if any) arising out of the Review. In doing so, have regard to what the applicant has asked for and what the recommendations of the PPIP Act are. If the Review does not propose to act on the applicant's request(s), explain why.*

Appendix 7

Checklist for internal review

Reference number(s): _____

This form is to be completed by the staff member overseeing the application for internal review.

1. Is the complaint a matter which involves a possible breach of the Privacy and Personal Information Protection Act, the Health Records and Information Privacy Act or a code made under these Acts?

If no, address via normal complaints handling process.

2. Date of receipt of application for internal review ___ / ___ / ___
3. Date when 60 calendar day period for completion of the review will elapse ___ / ___ / ___
4. Date when the Privacy Commissioner was notified of the request and invited to make submissions ___ / ___ / ___
5. Has the applicant provided the necessary information as required under section 53(3) of the Privacy and Personal Information Protection Act? Yes / No
6. Identify the relevant Information Privacy Principle, or Health Privacy Principle, or other section of either Act or code.

7. Name of Reviewing Officer _____
Position _____
Telephone number _____

8. Preliminary comments in relation to the application (attach response/submission from Privacy Commissioner)

9. Summary of the outcome of the review (attach recommendations from review)

10. Date that the applicant was notified of the outcome of the review, the proposed action and their right to seek a review of the findings within 28 calendar days of the review being completed (attach letter to applicant).
___ / ___ / ___

Name of Privacy Contact Officer (if different from Reviewing Officer) _____

