NSW Health Privacy Internal Review Guidelines

Summary These Guidelines help staff navigate and comply with all legislative requirements in conducting a privacy internal review.

Document type Guideline

Document number GL2019_015

Publication date 13 December 2019

Author branch Legal and Regulatory Services

Branch contact (02) 9391 9606

Replaces GL2006_007

Review date 13 December 2024

Policy manual Health Records and Information Manual for Community Health Facilities

File number H19/34499

Status Active

Functional group Clinical/Patient Services - Governance and Service Delivery, Records
Corporate Administration - Governance, Information and Data, Records
Personnel/Workforce - Conduct and ethics

Applies to Ministry of Health, Public Health Units, Local Health Districts, Board Governed Statutory Health Corporations, Chief Executive Governed Statutory Health Corporations, Specialty Network Governed Statutory Health Corporations, Affiliated Health Organisations, NSW Health Pathology, Public Health System Support Division, Cancer Institute, Community Health Centres, Dental Schools and Clinics, Public Hospitals, Environmental Health Officers of Local Councils

Distributed to Ministry of Health, Public Health System, Divisions of General Practice, Government Medical Officers, NSW Ambulance Service, Environmental Health Officers of Local Councils, Health Associations Unions, Tertiary Education Institutes

Audience All Staff of NSW Health

Secretary, NSW Health

GUIDELINE SUMMARY

PRIVACY INTERNAL REVIEW GUIDELINES

PURPOSE

NSW privacy law establishes a process of internal review for handling a privacy complaint, in certain circumstances.

These Guidelines help staff navigate and comply with all legislative requirements in conducting a privacy internal review.

Guidance is provided on undertaking an appropriate investigation into the privacy complaint, including conducting interviews and consultation requirements.

The Appendices include template letters and reports to provide practical assistance to staff, and a consistent approach to privacy complaint handling for NSW Health agencies.

KEY PRINCIPLES

60-day time limit

A privacy internal review must be completed as soon as practicable, and a time limit of 60 calendar days applies. The 60-day time limit starts from the receipt of the first written privacy complaint or request for privacy internal review. In exceptional circumstances, the agency may ask the applicant for an extension of time. (*Sections 5.3 and 5.4*)

NSW Privacy Commissioner

The NSW Privacy Commissioner must be notified of all applications for privacy internal review, provided with a draft investigation report for comment, and provided with the final report and covering letter to the applicant. (*Sections 5.7 and 7.3*)

NSW Civil and Administrative Tribunal

An individual who is dissatisfied with the outcome of the agency's privacy internal review, can lodge an application for administrative review with the NSW Civil and Administrative Tribunal (NCAT). This must be lodged within 28 calendar days of receipt of the privacy internal review report from the NSW Health agency. (*Section 7.1*)

USE OF THE GUIDELINE

Chief Executive

The Chief Executive, or their Senior Executive delegate, is ultimately responsible for the privacy internal review process and outcome. The Chief Executive, or their Senior Executive delegate, should approve the final internal review report and letter to the applicant. (*Section 3.4*)

Privacy Contact Officer, NSW Health agency

Privacy internal review is normally undertaken by the Privacy Contact Officer for the NSW Health agency. Privacy internal review must be undertaken without bias, and by an officer who is neutral to the circumstances relating to the complaint. If an officer was substantially involved in the matter relating to the complaint, including attempts to informally resolve the complaint, they are unable to undertake the privacy internal review. In such case, an alternative review officer must be appointed. (*Section 3.4 and 5.1)*

Ministry of Health

The Privacy Contact Officer, Ministry of Health and legal officers within the Legal and Regulatory Services Branch, may assist agency staff with matters of privacy internal review.

NSW Health agencies should:

- notify relevant privacy internal review matters to the Ministry, (*Section 5.5*)
- seek advice and clarification from the Ministry as necessary, (*throughout*)
- provide the draft internal review report to the Ministry for comment, (*Section 6.2*)
- provide final letter and internal review report to the Ministry, (*Section 6.4*)
- report statistical data on privacy internal reviews in the agency's privacy annual report (*Section 7.2*)

REVISION HISTORY

Version	Approved by	Amendment notes
December-2019 (GL2019_015)	Deputy-Secretary, People, Culture and Governance.	Expanded to include guidance on undertaking investigations, procedural fairness, and, where appropriate, referral to Human Resource departments.
May-2006 GL2006_007	Director, Legal and Legislation	New guideline in compliance with the *Privacy and Personal Information Protection Act 1998*, and the *Health Records and Information Privacy Act 2002*.

ATTACHMENTS

1. NSW Health Privacy Internal Review Guidelines

NSW Health Privacy Internal Review Guidelines

GUIDELINE

Issue date: December-2019

GL2019_015

CONTENTS

1 GLOSSARY

eMR	Electronic medical record
Health record	A documented account, whether in paper or electronic form, of a patient's health, illness and treatment during each visit or stay at a health service or an episode of care. Health record has the same meaning as medical record, clinical record and patient record.
Health service	A public health organisation (including a Local Health District, Specialty Network or Affiliated Health Organisation), a statutory health corporation, Ambulance Service of NSW, and units of the Health Administration Corporation that provide health services as part of the NSW public health system.
HPPs	The Health Privacy Principles (HPPs) established under the *Health Records and Information Privacy Act 2002*. There are 15 HPPs set out in Schedule 1 of the Act.
HRIP Act	*Health Records and Information Privacy Act 2002* (NSW)
ICAC	Independent Commission Against Corruption
IPC	NSW Information and Privacy Commission
IPPs	The Information Protection Principles (IPPs) established under the *Privacy and Personal Information Protection Act 1998.* There are 12 IPPs set out in Division 1 of the Act.
Must	The word 'must' indicates a mandatory action. Compliance with the requirement is mandatory.
NCAT	NSW Civil and Administrative Tribunal (NCAT). An applicant may apply to the NCAT to appeal the privacy internal review decision made by a health service.
PCO	Privacy Contact Officer
PPIP Act	*Privacy and Personal Information Protection Act 1998* (NSW)
Review Officer	Officer responsible for conducting the internal review. The Review Officer is usually the PCO, but may be another officer.
Should	The word 'should' indicates a recommended action that should be followed unless there are sound reasons for taking a different course of action.

2 INTRODUCTION

It is important that privacy concerns are appropriately managed by health services. A prompt and respectful response to individuals who raise privacy complaints is an important aspect of maintaining public confidence and trust in health services.

The aim of these Guidelines is to support NSW Health staff to comply with all legislative requirements in conducting privacy internal reviews. These Guidelines apply when a health service undertakes a privacy internal review in accordance with NSW privacy legislation.

This Guideline:

- Provides an overview of the legislative framework for privacy review and the role of Privacy Contact Officers / Review Officers.
- Addresses the application for privacy internal review, including what determines a valid application and the time limit for submitting an application.
- Provides guidance on the conduct of the privacy internal review, including conducting interviews and consultation requirements.
- Addresses the drafting of the privacy internal review report.
- Explains the applicant's right to appeal, annual reporting requirements and the role of the NSW Privacy Commissioner.
- Provide references, a flow chart and pro forma letters to assist the Privacy Contact Officer / Review Officer to meet legislative requirements when conducting a privacy internal review.

3 BACKGROUND

3.1 NSW privacy laws

NSW privacy laws govern the management of personal information held by public sector agencies in NSW. The two NSW privacy laws are:

- *Health Records and Information Privacy (HRIP) Act 2002 (NSW)*
- *Privacy and Personal Information Protection (PPIP) Act 1998 (NSW)*

The HRIP Act governs personal health information. In NSW Health, this mostly comprises patient health records. The HRIP Act sets out 15 Health Privacy Principles.

The NSW Health *Privacy Manual for Health Information* provides staff with guidance on how to comply with the Health Privacy Principles with respect to health information.

The PPIP Act governs all other 'non-health' personal information. In NSW Health, this mostly comprises employee records. The PPIP Act sets out 12 Information Protection Principles.

The NSW Health *Privacy Management Plan* provides guidance on how to comply with the requirements of the Information Protection Principles.

The provisions for privacy internal reviews are set out in Part 5 of the PPIP Act. These provisions apply to privacy internal reviews of alleged breaches under both the HRIP Act and the PPIP Act. These Guidelines reflect these legislative provisions.

3.2 When is an internal review required?

A request for a privacy internal review can be made where an individual believes that a health service has:

- breached any of the Health Privacy Principles, or
- breached any of the Information Protection Principles, or
- breached any code of practice or public interest direction made under either of the Acts applying to the health service, or
- disclosed information on a public register, except in accordance with section 57 (PPIP Act only).

A health service that receives a complaint from an individual who is aggrieved by the handling of their personal or health information is required to consider whether to undertake a privacy internal review. A privacy internal review must be conducted if the complaint is in the form of a valid application (see section 4.1).

An individual may also complain on behalf of someone else if they are authorised to act on their behalf. In addition, an individual may be aggrieved by the handling of someone else's personal or health information and such a complaint may also require a privacy internal review (see section 4.2).

Often the individual's initial complaint will not be in the form of a privacy internal review application. Nonetheless, if an individual expresses dissatisfaction with the handling of personal or health information, a health service must provide the person with information on their right to request a privacy internal review, and the requirements for lodging a valid application.

3.3 When is an internal review not required?

There may be circumstances where an internal review is not the appropriate response after an individual raises privacy concerns. Examples include:

- A person may raise general concerns about a health service's systems for handling health information. The health service may wish to address the person's concerns by reference to information management policies rather than through a privacy internal review process.

- A patient may express concern about the number of staff accessing their medical record. The patient may be satisfied with an explanation about the clinical rationale for staff accessing the record and reassurance regarding staff duties of confidentiality.
- An individual may have a query or request regarding access to a medical record. They may be satisfied for it to be resolved with a simple action, without a detailed internal review. For example, a complaint may arise because a request for access to or amendment of the patient's medical record was mistakenly refused. An internal review may not be necessary if access to or amendment of the record is uncontroversial and easily rectified.

In these scenarios, privacy internal review is not the appropriate response. Either the information does not relate to the individual making the complaint, the person is not aggrieved by the handling of their information, or the complainant does not want a privacy internal review.

3.4 The Chief Executive and Privacy Contact Officer roles

The health service's Chief Executive is ultimately responsible for the handling of a privacy complaint. The Chief Executive is required to nominate a person to act as Privacy Contact Officer (PCO) for that health service. Chief Executives or their delegate, other than the PCO or Review Officer, should approve the final privacy Internal Review Report before the report is sent to the applicant.

The health service's PCO is responsible for overseeing privacy complaints, including privacy internal reviews, in accordance with these guidelines.

Contact details for PCOs are available on the NSW Health *patient privacy webpage*.

It is usual practice for the PCO to conduct the internal review unless the PCO has a conflict of interest or is otherwise directed by the Chief Executive. Should an officer other than the PCO be nominated to conduct the privacy internal review, they may be referred to as the Review Officer for the purposes of conducting the review.

The PCO must also keep statistical data about the number of internal review requests received for annual reporting purposes (see section 7.2).

Staff should consult with the PCO regarding privacy queries and complaints they receive about breaches of privacy.

Privacy-related complaints may also be part of a clinical or governance-related complaint made to another department or unit within the health service. Human resource departments often handle staff grievances which may include privacy concerns. Staff of these departments or units should notify their PCO of all privacy-related matters. The PCO will then be able to determine whether the complaint, or a part thereof, should be handled as a privacy internal review. Similarly, an Internal Audit

Unit may become aware of privacy issues during audits or other investigations. When identified, issues should be referred to the PCO for consideration.

The Chief Executive is responsible for ensuring that a framework is in place to manage privacy training for staff. The framework should ensure that all staff undertake the mandatory privacy training module, and that all staff with access to clinical information systems have been appropriately trained and have signed privacy undertakings acknowledging that they understand their privacy obligations as NSW Health employees.

3.5 Informing the public about privacy internal review

Health services are required to inform the public about their privacy policies and procedures, including how to make a privacy complaint and the process of privacy internal review.

Requests for information about the internal review process should be directed to the health service's PCO or Chief Executive. A pro forma *Information Sheet for Privacy Internal Review*, which includes information about the requirements for requesting an internal review, is set out in Appendix 3. This information sheet should be adapted by the health service to include its name and contact details and should be provided to individuals requesting information about the privacy internal review process.

The NSW Health *Privacy Leaflet for Patients* provides contact details of PCOs for patients who have a privacy complaint. To obtain copies of this leaflet, contact the health service's PCO.

Both the *Privacy Leaflet for Patients* and *Information Sheet for Privacy Internal Review* should be sent to individuals requesting internal review.

4 THE APPLICATION

4.1 A valid privacy internal review application

Part 5 of the PPIP Act requires that an application for internal review of an alleged breach under either the HRIP Act or the PPIP Act must:

- be in writing
- be addressed to the agency (i.e. the relevant health service)
- 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 6 months from the time the applicant first became aware of the conduct. The agency may allow an extension of time in special circumstances (discussed in section 4.4 below).

4.2 Applicant must be aggrieved

An application for internal review can only be made by a person who is "aggrieved" by the conduct of the health service in relation to their information privacy, or by an authorised representative of that aggrieved person.

An aggrieved person 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 or a person might be aggrieved about a breach of their elderly parent'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 health service should assess the application to identify if this person has been directly affected by the alleged breach. Consideration should then be given to what extent, if any, it would be appropriate to provide information about the patient to the applicant.

The HRIP Act sets out the list of people who can be an authorised representative of a patient who lacks capacity. It is generally necessary to review a patient's health record to determine who is their authorised representative. Personal identification and other documentation relating to the person's role as an authorised representative (e.g. enduring power of attorney, guardianship documents, proof of relationship status) should be provided with the application. If a person has capacity, an authorised representative can lodge an application for internal review on the person's behalf if the person expressly authorises the authorised representative to do so (e.g. a signed and dated consent or authority). For more information, see section 5.6 of the NSW Health Privacy Manual for Health Information.

4.3 Privacy internal review application form

The NSW Health *Privacy Internal Review Application Form* is provided in Appendix 4. Applicants may also use an alternative privacy complaint form, such as the form provided by the NSW Information and Privacy Commission.

It is not obligatory for applicants to complete a form. It is sufficient for their complaint to be received in writing (e.g. letter or email). However, the application form can be useful for both the applicant to articulate their complaint and for the health service to gain a more detailed understanding of the complaint. Therefore, this form should be provided to applicants where possible. A pro forma letter requesting completion of the form is provided at Appendix 5.1.

The PCO should always contact the complainant prior to initiating an internal review, to ensure that all issues that may assist the internal review have been identified.

4.4 Extension of 6-month time limit

An application for privacy internal review must be lodged within 6 months from the time the applicant first became aware of the conduct which their complaint relates to. If the time frame is over 6 months, the application is considered 'out of time'. If the date at which the applicant became aware of the conduct which is the subject of the complaint is unclear in the application, clarification should be sought from the applicant before proceeding with any aspect of the internal review process.

The health service may exercise its discretion to extend the time for receiving internal review applications beyond the 6-month period. In determining whether to accept an application made after the 6-month period, the health service may consider:

- the length of the delay
- the merits of the complaint
- whether the complainant can demonstrate a reasonable explanation for the delay, such as ill-health, family trauma or other reasons relating to incapacity.

An applicant should always be offered the opportunity to explain the delay before a decision is reached to decline an application. This will be relevant in circumstances where the applicant's complaint has been received via an email or letter instead of via an Information and Privacy Commission (IPC) or NSW Health privacy internal review application form (which provide the applicant with an opportunity to explain any delay).

If an applicant has not provided a reason for the delay (in a NSW IPC or NSW Health privacy internal review application form) they do not need to be provided with another opportunity to explain the delay and it can be presumed there is no reasonable explanation. On this basis, a decision not to extend time can be made by the health service.

Any decision to extend time for an applicant should be made in consultation with the Ministry of Health's Privacy Contact Officer.

If a decision is made not to extend the time for receiving the application beyond the 6-month period, the health service should inform the individual of this decision. A pro forma letter is provided at Appendix 5.2. The health service must also notify the NSW Privacy Commissioner that the application was received and declined on the basis that it was out of time and provide the NSW Privacy Commissioner with a copy of the application.

The health service's response to the issues raised in such an out of time application may vary depending on the circumstances. The health service's Privacy Contact Officer should consider whether further action is required in relation to the conduct complained about. The Privacy Contact Officer will undertake an assessment of the concerns raised by the complaint to determine whether any management action should be taken in response. The complainant would normally be informed of the outcome of such an assessment.

Where the complaint is not privacy-related, or includes other matters, it should be referred to the appropriate complaint handling staff of the health service.

Where the complaint has already been addressed within the health service, the Privacy Contact Officer may refer the applicant to the NSW Information Privacy Commission (IPC) to help address the complaint.

In complex matters, the Privacy Contact Officer may liaise with the Ministry of Health's Privacy Contact Officer to discuss the health service's response.

4.5 Anonymised applications for internal review

In some circumstances, an applicant may want their letter of complaint or internal review application anonymised when it is provided to the NSW Privacy Commissioner. The Privacy Contact Officer should carefully review the application to assess whether there is any indication that anonymity should be preserved. While an internal review can be completed this way, the applicant should be informed that disclosure of their personal details will be required if they wish to apply for a further review by the NSW Civil and Administrative Tribunal (NCAT). The standard application form includes an option for the applicant to request that all identifying information be withheld from the NSW Privacy Commissioner.

It may also be preferable to anonymise the identity of NSW Health staff members and other third parties who are witnesses to the conduct which is the subject of a complaint (see section 5.11).

If the applicant and witnesses are anonymised in the internal review, their identities should be documented by the health service in its internal file notes. For example:

- John Brown – The Applicant
- Sarah Clarke – Witness A

5 CONDUCTING THE PRIVACY INTERNAL REVIEW

5.1 Review Officer

The privacy internal review must be conducted by a Review Officer. It is a requirement of the PPIP Act that this officer must be, as far as 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 health service; and
- is otherwise suitably qualified to deal with the matters raised by the application.

In most cases, the Review Officer will be the health service's PCO. A person may be considered substantially involved if they had 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. This includes involvement in attempts to informally resolve the complaint. In complaints such as these, the PCO should declare a conflict of interests and recuse themselves from any review of the matter.

Where the PCO is unable to undertake the privacy internal review, the Chief Executive, or delegate, must appoint another internal officer capable of undertaking a fair and unbiased internal review, in accordance with these guidelines. Where difficulties arise, guidance can be sought from the Privacy Contact Officer, Ministry of Health, to assist in selecting a suitable alternative Review Officer.

The PPIP Act allows for the applicant to request that the NSW Privacy Commissioner undertake a privacy internal review. However, in practice, it would be extremely rare for the NSW Privacy Commissioner to undertake this role in relation to a health service.

5.2 Acknowledging receipt of application

When an internal review application is received by a health service, it must be promptly forwarded to the health service's PCO for review. The PCO must consider whether it is a valid application for privacy internal review (see 4.1 and 4.2).

If the PCO accepts the application as valid, the PCO should send a letter of acknowledgement of receipt of the application to the applicant with an information sheet for privacy internal review. A pro forma letter acknowledging receipt of the application is provided at Appendix 5.1.

Where appropriate, before sending the letter of acknowledgement to the applicant, the PCO or Review Officer may contact the applicant by telephone or email to gather further information about the nature of their complaint. This can be particularly useful if the applicant has only provided brief comments as part of the standard application form. It will also assist the Review Officer to identify which privacy principles may have been breached and provide an opportunity to manage the applicant's expectations.

5.3 60-day time limit to complete the review

The Review Officer must complete the review as soon as reasonably practicable in the circumstances. There is a time limit of 60 calendar days for completing the review. The 60-day time limit starts from the receipt of the first written privacy complaint or request for privacy internal review, regardless of whether an application form is used. The PPIP Act allows an additional 14 days for the health service to notify the applicant of the findings and recommendations, in exceptional cases.

To ensure completion of the internal review within this time limit, the Review Officer should prepare a work plan that allocates sufficient time over the 60-day period for all steps involved, including:

- 1 to 2 weeks for gathering and reviewing documents and interviewing the applicant and individuals who can assist with providing information for the review.
- 1 to 2 weeks to prepare the draft report, including the review of relevant records, and reference to relevant policy and procedures.
- 1 week for consideration of the draft report by the Ministry of Health and amending the draft in response to feedback.
- 2 weeks for consideration of the draft report by NSW Privacy Commissioner, Information and Privacy Commission and to amend the draft in response to feedback.

Provision of the final report to the applicant must be within the 60-day time period, unless permission is obtained from the applicant to extend. In exceptional cases, an additional 14 days may be allowed for postage.

5.4 Reviews not completed within 60 days

The review must be completed as soon as is reasonably practicable in the circumstances. If the health service foresees that completion of the review will take longer than 60 calendar days, the Review Officer should advise the applicant in advance, explaining why 60 days was insufficient in the circumstances, and inform the applicant of the expected completion date.

If the review has not been completed within 60 calendar days, the applicant is entitled to make an application to the NCAT for a review of the privacy complaint. The applicant must be informed of this when they are advised of any delay in the completion of the report. See the pro forma letter at Appendix 5.3.

5.5 Notification to the Ministry of Health

5.5.1 Complaints about health information under the HRIP Act

The management of health information is a fundamental function of the NSW public health system.

Privacy complaints may have broader system-wide implications for NSW Health, along with decisions appealed in the NCAT. For this reason, it is important that the Ministry of Health's Privacy Contact Officer is notified in writing of all privacy internal reviews under the HRIP Act.

The Ministry of Health's Privacy Contact Officer may assist NSW health services in all matters relating to the administration of the HRIP Act.

Notification to the Ministry of Health can be addressed to:
MOH-Privacy@health.nsw.gov.au

5.5.2 Complaints about personal information under the PPIP Act

Notification of privacy internal review matters under the PPIP Act is different to the HRIP Act.

In most cases, other than for significant legal matters (see section 5.6), privacy internal reviews in relation to complaints about personal information under the PPIP Act will not have significant impacts across the health system. It is appropriate for these matters to be managed locally by the health service.

The reporting and time frame requirements for PPIP Act applications are the same as those that apply to the HRIP Act.

Where health services require guidance regarding a PPIP Act internal review, they may discuss the matter in general terms with the Ministry of Health's Privacy Contact Officer. However, care needs to be taken in the management of the applicant's personal information. In PPIP Act matters, health services should not disclose identifying information about the applicant to the Ministry of Health, other than to the Ministry's legal team for "significant legal matters" (see section 5.6).

If an application for internal review contains both HRIP Act and PPIP Act complaints, liaison with a Ministry of Health Privacy Contact Officer or Legal Officer should occur before releasing any personal information to the Ministry.

5.6 Significant legal matters

If an internal review under either the HRIP Act or PPIP Act involves a "significant legal matter", it should be notified to the Ministry of Health legal team, following consultation with the Chief Executive (or delegate). "Significant legal matters" include:

- Matters that raise issues fundamental to the responsibilities of the Minister for Health, Health Secretary, Ministry of Health, Health Administration Corporation, or any officer thereof.
- Significant medico-legal, ethical, policy, industrial, work health and safety or other operational issues. For example, matters relating to allegations of historical sexual abuse.

- Legal proceedings to which a NSW health service or its officers are a party, which raise a significant question of interpretation of policy or legislation administered by the Minister for Health.
- Legal proceedings involving more than one NSW health service, multiple NSW Government agencies, or a Minister of the Crown. Legal engagement involving the expenditure, or reasonably anticipated expenditure, on legal costs and disbursements in excess of $150,000.

Further details are set out in the NSW Health Policy Directive *Significant Legal Matters and Management of Legal Services* (PD2017_003).

To notify of a significant legal matter, email the Ministry of Health legal team at: MOH-SignificantLegalMatters@health.nsw.gov.au

5.7 Notifying the NSW Privacy Commissioner

The PCO or Review Officer must write to the NSW Privacy Commissioner to advise that an application for internal review has been received, and to provide a copy of the application. The application form allows the applicant to request that the health service withhold identifying information from the NSW Privacy Commissioner. See Appendix 6 for a pro forma letter of notification to the NSW Privacy Commissioner.

The Ministry of Health's PCO must be copied into all correspondence to the NSW Privacy Commissioner relating to internal reviews under the HRIP Act.

5.8 Steps in an internal review

An internal review may involve:

- seeking further information from the applicant
- reviewing internal health service records or other documents, including relevant sections of the applicant's medical record or other material held by the service relevant to the application
- referring to relevant NSW Health policies and relevant local procedures to determine whether staff involved in the complaint acted in accordance with these policies and procedures
- interviewing staff or other individuals involved in the conduct which is the subject of the complaint
- running an eMR audit against the patient's name and against the staff member's name
- checking with the applicant as to whether other privacy complaints have been made to the health service. A privacy complaint is sometimes included in a general complaint, for example, a complaint made to a Patient Complaints Officer or the Workforce Services (Human Resources) Unit. Any prior complaints regarding the same matter should be documented in the Internal Review Report as background.

5.9 Procedural fairness

Procedural fairness must be afforded to staff who are the subject of the internal review.

Information must be provided to the staff member about the complaint and any allegations made against him or her. The Review Officer should also explain the review process to the staff member. Information about the complaint should be detailed enough to allow the staff member to provide a considered response. If the person is to be interviewed, the person should be provided at least 48 hours' notice.

Procedural fairness requires that a person who is the subject of review must be given an opportunity to respond to adverse findings made against them before any disciplinary action is taken. The Review Officer must act impartially and without bias when undertaking an internal review.

As in all matters, care must be taken to maintain the confidentiality of the applicant and third parties involved in the matter. When interviewing staff, they should be reminded of their duties of confidentiality in relation to the complaint. This does not preclude them from seeking advice from their union or a support person.

The final Internal Review Report should not be provided to the staff member who is the subject of the complaint. However, the staff member should be permitted to review and comment on any statements attributed to them or transcripts from records of interview. If necessary, a staff member may review excerpts of a draft report, to verify factual matters.

Affected staff should be informed about any adverse findings relevant to them. In the event that multiple staff have been interviewed for an internal review, care needs to be taken to ensure the confidentiality of each staff member is respected and maintained.

If the concerns raised in the internal review application involve possible staff misconduct, the Review Officer should consult with Workforce Services/Human Resources before contacting the staff member. In such cases, the privacy internal review may need to proceed concurrently with a misconduct investigation under the NSW Health *Managing Misconduct Policy Directive* (PD2018_031). Further guidance is provided below in sections 5.14 and 5.15.

For further information, see:

- NSW Ombudsman, *Investigating complaints: A manual for investigators*
- NSW Ombudsman, *Good conduct and administrative practice - Guidelines for state and local government*

5.10 Interviewing the applicant

Interviewing the applicant can be of assistance to clarify the precise nature of the concerns held by the applicant. Often applicants can better explain their complaint

verbally than in writing. When practicable, interview the applicant in person. All attempts to contact the applicant should be documented.

Prepare a list of questions to ask the applicant at the interview. Key issues to consider when interviewing the applicant include:

- Does any of the information in the application require clarification?
- Is any information missing?
- What other information do we need to collect as part of a diligent review?
- Are there individuals inside or outside the health service who should be contacted about the complaint? How can they be contacted?
- Has the applicant already complained about the conduct before submitting their application for internal review? If so, to whom was the complaint made and what was the response?

During the interview, the Review Officer should explain to the applicant the process for internal review and the actions that can be taken by the health service to resolve the applicant's concerns. The Review Officer should manage the applicant's expectations and explore what outcome they are seeking, then indicate what action may be taken by the health service. The Review Officer should not commit the health service to undertake specific actions before the investigation is finalised and the decision-maker has reviewed the Internal Review Report.

5.11 Interviewing others

As far as practicable, interviews should be conducted in person. The Review Officer should interview the applicant, then relevant staff members who can assist in providing information, and then the staff member(s) the subject of the complaint. In rare circumstances, interviews may also be conducted with other patients or members of the public who may have witnessed or been involved in the incident that gave rise to the complaint.

A staff member who is the subject of a complaint should be advised of the nature of the complaint, the internal review process and any relevant evidence that has been provided in the complaint, or obtained during the review, such as eMR audit reports, the staff privacy undertaking and emails. Once the Internal Review Report has been finalised, the staff member should be advised of the findings.

All staff members who are interviewed for an internal review should be provided with a copy of the Information Sheet for privacy internal review (see Appendix 3) and NSW Health *Privacy Leaflet for Staff* (see section 8).

Staff who are interviewed should review any records of interview or statements to ensure that they accurately reflect their version of events. Confirmation from the staff member that the record is accurate may be obtained by email or signature on the statement. Although written confirmation of accuracy of the record is not a strict

requirement, it is helpful because if the applicant appeals to NCAT, staff will need to prepare affidavits detailing their version of events.

Under the NSW Health *Code of Conduct* it is expected that staff will assist in the interview process. If a person does not agree to participate in an interview, the Review Officer should make a contemporaneous note as to their concerns and the reason why they have declined to participate and discuss the issue with Human Resources.

If relevant staff have left the organisation, and they are important witnesses, they may be invited to participate in an interview. However, this should only be done with the approval of a senior officer.

In some circumstances the Review Officer may consider it appropriate to anonymise the identities of staff in the report taking into account the public interest considerations against disclosure, having regard to the principles in section 14 of the *Government Information Public Access Act 2009*. For example, this might be because:

- the applicant or the applicant's family have made threats of violence to the staff member
- the report raises workplace relations issues
- staff reside in small rural communities where managing confidentiality can be challenging
- there are other investigations or legal matters being conducted at the same time
- the applicant is a staff member.

Advice on anonymising staff identities can be sought from the Ministry of Health.

Occasionally, patients or other members of the public may also be approached as witnesses. Consideration should be given as to whether contacting these individuals is reasonable having regard to the seriousness of the complaint and how long ago the events occurred. Any decisions that are made about how to proceed and the reasons for those decisions should be documented in a file note and retained as part of the internal review file.

Sometimes the applicant may be opposed to involving other people who may have information that would assist the review. If the Review Officer believes that approaching these individuals would assist in confirming a breach of privacy, it should be explained to the applicant that if the individuals are not contacted it may affect the outcome of the review. If the applicant insists that they not be contacted, this should be documented in the Internal Review Report, so it is clear to the NSW Privacy Commissioner why certain aspects of the complaint were not investigated by the health service.

Members of the public are not obliged to assist in an internal review and their participation is voluntary. All attempts to approach members of the public should be

documented. Advice from a senior executive should be sought prior to initiating such contact.

If a member of the public does not agree to participate in the internal review, their identity should be anonymous in the Internal Review Report. However, the personal details of potential witnesses should be recorded separately, so that they can be contacted if their information later becomes relevant to NCAT proceedings.

5.12 Has the health service breached a health privacy or information protection principle?

In light of the information gathered through the internal review, the Review Officer must identify which (if any) Health Privacy Principles (HPPs) under the HRIP Act, or Information Protection Principles (IPPs) under the PPIP Act have been breached.

Where it is suspected that a staff member has breached an HPP or an IPP, the Review Officer must determine the nature and extent of the breach including if it was deliberate or accidental.

The Review Officer may wish to consult with a Ministry of Health PCO to ensure the correct privacy principles have been identified.

Issues that may require consideration include:

- Was the personal or health information used or disclosed without authority? (HPPs 10/11 and IPPs 10/11)
- Would the applicant have a reasonable expectation that their health information would be used by the health service in this way? (HPP 10 (1)(b) and HPP 11(1)(b))
- What evidence is there that the applicant was informed about the use of their information? (HPP 4 and IPP 3)
- Was the applicant given appropriate access to their records? (HPP 7 and IPP 7)
- Was the applicant aware that their personal or health information was being collected? (HPP 3 and IPP 2). If not, was the information lawfully collected? (HPP 1 and IPP 1)
- Is the information held about the applicant accurate? (HPP 9 and IPP 9)
- Was the information held securely? (HPP 5 and IPP 5)

5.13 Has the privacy of other persons been breached?

In some circumstances, an application for privacy internal review may identify system failures or breaches that may impact on the privacy of persons other than the applicant. There is no legal obligation under the HRIP Act or any other NSW legislation for the health service to notify such other persons if their privacy has been breached.

However, as a matter of good practice, a risk assessment should be conducted to determine whether the affected persons should be notified.

In general, affected persons should be notified if sensitive personal information has been made publicly available (e.g. via the internet), or if there is a risk of serious harm as a result of a breach. Risk of harm can include psychological, physical, financial or other harm. The health service should notify the Ministry of Health, and consideration should be given as to whether the NSW Privacy Commissioner should be notified. The NSW Information and Privacy Commission has published resources to assist agencies to determine whether there is serious risk of harm including Data Breach Guidance and a data breach notification form.

Where the matter relates to a breach involving a person's health information held in the My Health Record, the health service must notify the Australian Digital Health Agency (ADHA) in the first instance.

For further information, see:

- NSW Information and Privacy Commission, *Data Breach Guidance*
- NSW Information and Privacy Commission, *Data Breach Notification form*
- Australian Digital Health Agency (ADHA), *My Health Record Data Breach Notification Steps*

5.14 Is consultation required with Workforce Services (Human Resources)?

If the circumstances indicate there has been a deliberate breach of privacy, assessment will be required to determine whether to also manage the review under the NSW Health *Managing Misconduct Policy Directive* (see below). The Review Officer should consult with Workforce Services (Human Resources), Internal Audit or an appropriate senior executive to determine how to manage the privacy internal review concurrently with a misconduct investigation.

The *Managing Misconduct Policy Directive* (PD2018_031) defines misconduct to include:

- Conduct which seriously or repeatedly breaches expected standards, as identified in relevant legislation or NSW Health policies
- Reportable (i.e. child-related) conduct as defined under the *Ombudsman Act 1974*
- Corrupt conduct under the *Independent Commission Against Corruption Act 1988*

Misconduct, therefore, includes serious or repeated breaches of the HRIP Act, *NSW Health Code of Conduct* or the *Privacy Manual for Health Information*. Examples of serious breaches include where a staff member has accessed the records of colleagues or multiple family members, or where there is a pattern of behaviour rather than an isolated incident, sharing personal or health information about a patient or

colleague on social media or online, or where the information contained in the record is particularly sensitive such that a privacy breach may result in harm to the person affected.

The Review Officer should consult with a Ministry of Health PCO if the Review Officer is uncertain about management of a privacy internal review involving suspected staff misconduct.

For further information, see:

- NSW Health Policy Directive, *Managing Misconduct PD2018_031*
- NSW Health Policy Directive, *Managing Complaints and Concerns about Clinicians PD2018_032*

5.15 Is consultation required with Internal Audit?

An intentional breach of privacy made by an employee falls under the provisions of the *Independent Commission Against Corruption Act 1988* (ICAC Act). Corrupt conduct, as defined in the ICAC Act, is deliberate or intentional wrongdoing, not negligence or a mistake. It has to involve or affect a NSW public official or public sector organisation.

The ICAC Act also imposes an obligation on Principal Officers of NSW Health organisations to report possible corrupt conduct to the ICAC.

If corrupt or criminal conduct is suspected, the Review Officer should liaise with Internal Audit and the Ministry of Health. Some intentional privacy breaches including misuse of electronic patient data may constitute criminal conduct.

Corrupt disclosure and use of information are criminal offences under section 68 of the HRIP Act and section 62 of the PPIP Act. These sections provide that staff must not, other than in the course of their employment, intentionally disclose or use any health information / personal information about an individual to which the staff member has access in the exercise of his or her official functions. The maximum penalty is a fine of $11,000 (100 penalty units), imprisonment for two years, or both.

For further guidance, see:

- NSW Health Information Sheet, *Reporting misuse of information as suspected corrupt conduct*
- NSW Health Policy Directive, *Corrupt Conduct – Reporting to the Independent Commission Against Corruption (ICAC) PD2016_029*
- NSW Health, *Privacy Leaflet for Staff*

5.16 Is consultation required with NSW Police?

Criminal offences in the HRIP Act, PPIP Act and/or the *Crimes Act 1900* may apply to staff for unauthorised access to or misuse of information.

There are statutory time limits that may impact on these complaints. It is very important that they are reported to NSW Police and the NSW Ministry of Health as soon as possible.

Section 308H of the *Crimes Act 1900* provides for an offence for unauthorised access to or modification of restricted data held in a computer. Proceedings for an offence against section 308H must be commenced **within 12 months** from when the offence was alleged to have been committed.

Most other summary offences (including the offences relating to corrupt disclosure or misuse of information under the HRIP Act and PPIP Act) must be prosecuted **within 6 months** of the offence.

Applicants need to be made aware of their rights to make a complaint to police before these time periods expire. Applicants should be advised to seek independent legal advice in relation to pursuing a prosecution.

Health services are required to liaise with a Ministry of Health PCO when referring any privacy matters to NSW Police or ICAC.

6 THE INTERNAL REVIEW REPORT

6.1 Content of the report

Appendix 8 provides an internal review report template to assist in the writing of the report. The report should include the following:

Background information

Background information on the facts and history of the complaint. A timeline that summarises the sequence of events may be helpful. Keep in mind that the report will be read by the office of the NSW Privacy Commissioner, who may not have the reviewer's knowledge of the health system. Make sure relevant policies and procedures are clearly set out.

A description of the review process (for example, list of interviewees, documents, records and policies referenced). Describe the approach taken to analyse the information and evidence that has been collected.

Findings of the review

The findings of the review including whether a privacy breach was found to have occurred, and the reasons for those findings. The report should clearly demonstrate to the applicant and the Privacy Commissioner how the reviewer has come to make the findings.

The findings should address whether more could have been done by the health service to prevent a privacy breach occurring.

Questions to consider may include:

- Were the health service's practices compliant with relevant NSW Health policy and legislative requirements?
- Has the health service implemented sufficient data security safeguards?
- Have staff received appropriate privacy training?
- Are audits conducted of staff access to electronic medical records?

Report recommendations

The report must recommend one or more of the following:

- Make a formal apology to the applicant (if a breach has been substantiated this should always occur).

- Take appropriate remedial action (for example, improve security controls, amend records, or consider offering compensation to the applicant, subject to authorisation by an officer with delegated authority).
- 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, introduction of new business rules or systems, and privacy training for relevant staff.
- Take no further action on the matter.

The report may include recommendations in relation to referral to Internal Audit. The report should not make a finding of criminal or corrupt conduct. However, if there is a concern that any conduct may be criminal in nature the report should make a recommendation that the matter be referred to Internal Audit to assess whether the conduct should be reported to ICAC or police.

The report should refer to the right of the person to have the findings of the review and the health service's proposed actions reviewed by the NSW Civil and Administrative Tribunal (NCAT).

6.1.1 Points to consider when writing the report

- Use plain language and avoid health system jargon and acronyms as far as possible. The report should be helpful to the applicant and provide open and transparent explanations of the circumstances surrounding the complaint.
- The report will be sent to the applicant, so care must be taken not to disclose personal information about any third parties.
- Any information provided on behalf of staff members should be accurate and consistent with their statements.
- If the applicant disagrees with the findings of the review, he or she may appeal to NCAT. If there is an appeal, the Internal Review Report will be submitted as evidence to NCAT, so it is essential that it reflects that a fair, unbiased, thorough and accurate review has taken place.
- Reference should be made to policies, procedures, records of signed privacy undertakings, privacy training records, audit reports, patient information leaflets and any other documents relevant to the circumstances of the complaint. This can help to clarify how personal information is managed by the NSW health system. For example, it may be useful to explain to an applicant the security measures in place to prevent unauthorised access to clinical information, including the signed undertakings and individual personal logins that are required.

6.2 Review of draft reports by the Ministry of Health and NSW Privacy Commissioner

The health service should provide the draft report to the Ministry of Health's PCO for review and comment. This should occur prior to sending the draft to the NSW Privacy Commissioner. This applies to all HRIP Act internal reviews reports and any PPIP Act internal reviews that are, or form part of, significant legal matters.

The Ministry of Health generally requires seven to ten working days to review a draft Internal Review Report, but if the matter is complex more time should be allowed.

The PPIP Act requires the health service to keep the NSW Privacy Commissioner informed of the progress of the internal review and to inform the Privacy Commissioner of the review findings and the action proposed to be taken by the health service in response to the findings. The Privacy Commissioner is entitled to make submissions (discussed at section 6.3 below) to the health service in relation to the application. In practice, this means the office of the NSW Privacy Commissioner requires a copy of the draft report before it is sent to the applicant.

The office of the NSW Privacy Commissioner generally requires at least two weeks to review a draft Internal Review Report.

See Appendix 7 for a pro forma letter / email providing the draft Internal Review Report to the NSW Privacy Commissioner.

6.3 Submissions from the NSW Privacy Commissioner

Any submissions received from the Privacy Commissioner should be taken into consideration when preparing the final report. The health service should provide the Ministry of Health's PCO with any submissions received from the NSW Privacy Commissioner in all HRIP Act internal reviews and any PPIP Act internal reviews that have been identified as addressing significant legal matters, to assist the health service in their consideration of their response to the submissions.

If the Review Officer has concerns about the submissions of the NSW Privacy Commissioner, they can be discussed directly with the office of the NSW Privacy Commissioner to gain a better understanding.

Under no circumstances should a health service provide an applicant with a copy of an internal review report prior to receipt of any comments or submissions from the NSW Privacy Commissioner, as the report may require amendment. Advice should be sought from the Ministry of Health's PCO, if this is a problem.

6.4 Issuing the final report

Following completion of the review, the health service must provide the applicant with the completed internal review report and covering letter (Appendix 5.4) as soon as

practicable or, in any event, within 14 days of completion (section 53(8) of the PPIP Act).

However, if there are extenuating circumstances and the report cannot be provided within the required timeframe, the officer should contact the applicant, explain the circumstances for the delay and request additional time to complete the review (see Appendix 5.3).

The health service 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 health service and the reasons for taking that action; and
- the right of the person to have those findings, and the health service's proposed action, reviewed by NCAT.

A copy of the final internal review report and covering letter sent to the applicant must be provided to the NSW Privacy Commissioner and the Ministry of Health.

7 APPEALS, ANNUAL REPORTING, AND ROLE OF THE NSW PRIVACY COMMISSIONER

7.1 Appeals to the NSW Civil and Administrative Tribunal (NCAT)

7.1.1 Lodging an NCAT application

If the applicant is dissatisfied with the outcome of the internal review, the applicant has a right to appeal to the NCAT within 28 calendar days from being notified of the findings of the internal review. The applicant must post the appeal form to the NCAT registry or deliver it in person. The appeal cannot be lodged online or by email.

If the appeal deadline has passed, the applicant can ask NCAT for an extension. It will be up to NCAT to decide at a directions hearing whether or not to accept a late application.

After accepting an appeal application, NCAT will notify the health service of the appeal and the date of the first planning meeting before a Registrar. As soon as this correspondence is received from NCAT, the health service must notify:

- the Privacy Contact Officer, Ministry of Health;
- the litigation contact in your health service (and/or your Chief Executive, as dictated by local policy); and
- Ministry of Health legal team, so that appropriate representation can be arranged for the planning meeting (email: MOH-SignificantLegalMatters@health.nsw.gov.au).

7.1.2 Legal representation

Any decision by the health service to appear without legal representation at the planning meeting should be discussed in consultation with the Ministry of Health legal team. In most circumstances, a solicitor will represent the health service. The Privacy Contact Officer or Review Officer who conducted the internal review will liaise with the health service's solicitor to prepare the matter for NCAT. The solicitor will require copies of all the statements, policies and other materials used in the preparation of the internal review. The appeal is a fresh administrative review of the complaint, so the solicitor may also request further information. This might mean that:

- witnesses may need to answer further questions
- additional statements may need to obtained
- further policies or documents may need to be provided.

As the case proceeds through NCAT processes from planning meetings and case conferences to the hearing date, the parties may attempt to resolve the complaint through negotiation.

7.1.3 NCAT orders

If the case proceeds to a hearing, NCAT may make one or more of the following orders after the hearing is completed:

(a) an order requiring the health service to pay to the applicant damages not exceeding $40,000 by way of compensation for any loss or damage suffered because of the conduct,

(b) an order requiring the health service to refrain from any conduct or action in contravention of an information protection principle or a privacy code of practice,

(c) an order requiring the performance of an information protection principle or a privacy code of practice,

(d) an order requiring personal information that has been disclosed to be corrected by the health service,

(e) an order requiring the health service to take specified steps to remedy any loss or damage suffered by the applicant,

(f) an order requiring the health service not to disclose personal information contained in a public register, or

(g) such ancillary orders as NCAT thinks appropriate.

Alternatively, NCAT may decide not to take any further action on the matter.

7.2 Annual reporting

All health services must complete an annual report on privacy. The report should be completed by 31 August and must be made publicly available on the website of each health service. Consideration should be given to co-locating privacy reports with other annual reports.

Requirements for annual reporting are set out in clause 6 of the *Annual Reports (Departments) Regulation 2015* and in clause 8 of the *Annual Reports (Statutory Bodies) Regulation 2015.* The annual report of each health service must include:

- a statement of the action taken by the health service in complying with the requirements of the PPIP Act and HRIP Act, such as the delivery of privacy training to staff and distribution of information regarding privacy to patients
- statistical data on any privacy internal reviews conducted by or on behalf of the health service.

The report should provide details of when the applications for review were received, and a summary of the outcomes. The summary should include:

- whether any privacy principles were breached, and the broad context of the breach
- whether the applicant sought further review in NCAT and a summary of any NCAT findings.

Care must be taken to ensure that the details included in the annual report in no way identify the applicant or other participants in the internal review.

7.3 Role of the NSW Privacy Commissioner

7.3.1 Monitoring progress

The NSW Privacy Commissioner has a monitoring role during the course of an internal review. After an application for internal review is received, the health service should:

- notify the Privacy Commissioner of the receipt of the application as soon as practicable (see Appendix 6),
- keep the Privacy Commissioner informed of the progress of the internal review,
- inform the Privacy Commissioner of the draft findings of the internal review and of the action proposed to be taken by the health service in relation to the matter (see Appendix 7), and
- provide the Privacy Commissioner with the finalised internal review report and covering letter to the applicant.

The health service should not release the findings of the privacy internal review to the applicant until the health service has received any submissions or comments from the Privacy Commissioner as this might lead to the report's amendment. Generally, the Privacy Commissioner's office requests a minimum of two weeks to review and respond to a draft report. The Privacy Commissioner can sometimes be delayed. If this happens it is important to keep the applicant informed of the delay. If the Privacy Commissioner's comments or submissions are delayed and an extension of time for completion of the internal review is required, the applicant should be advised via the standard extension letter (see Appendix 5.3).

7.3.2 Investigating privacy complaints

The NSW Privacy Commissioner can also receive and investigate privacy complaints received directly from individuals. This option exists separately from the right to an internal review.

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 to the Privacy Commissioner must be made within 6 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.

It is rare for the Privacy Commissioner to conduct such an investigation. In most cases, complaints are referred to the relevant health service for internal review.

8 REFERENCES

8.1 Legislation

Privacy and Personal Information Protection Act 1998 (NSW)

Health Records and Information Privacy Act 2002 (NSW)

Crimes Act 1900 (NSW)

Independent Commission Against Corruption Act 1988 (NSW)

My Health Records Act 2012 (Cth)

Ombudsman Act 1974 (NSW)

8.2 NSW Health

Ministry of Health Privacy Contact Officer email: MOH-Privacy@health.nsw.gov.au

NSW Health Patient privacy webpage

NSW Health Privacy Manual for Health Information

NSW Health Privacy Management Plan

NSW Health Privacy Leaflet for Patients

NSW Health Privacy Information for Staff

NSW Health Code of Conduct

PD2009_076 Communications - Use & Management of Misuse of NSW Health Communications Systems

PD2013_033 Electronic Information Security Policy - NSW Health

PD2016_029 Corrupt Conduct - Reporting to the Independent Commission Against Corruption

PD2017_003 Significant Legal Matters and Management of Legal Services

PD2018_031 Managing Misconduct

PD2018_032 Managing Complaints and Concerns about Clinicians

8.3 Information and Privacy Commission

NSW Information and Privacy Commission, Internal Review Checklist for the Respondent Agency

NSW Information and Privacy Commission, Protocol for handling privacy complaints

NSW Information and Privacy Commission, Data Breach Guidance

NSW Information and Privacy Commission, Data Breach Notification form

8.4 My Health Record

Australian Digital Health Agency (ADHA), My Health Record Data Breach Notification Steps

9 APPENDICES

Appendix 1 Flow chart of the internal review process

Appendix 2 Checklist for privacy internal review

Appendix 3 Information sheet for privacy internal review

Appendix 4 Privacy internal review application form

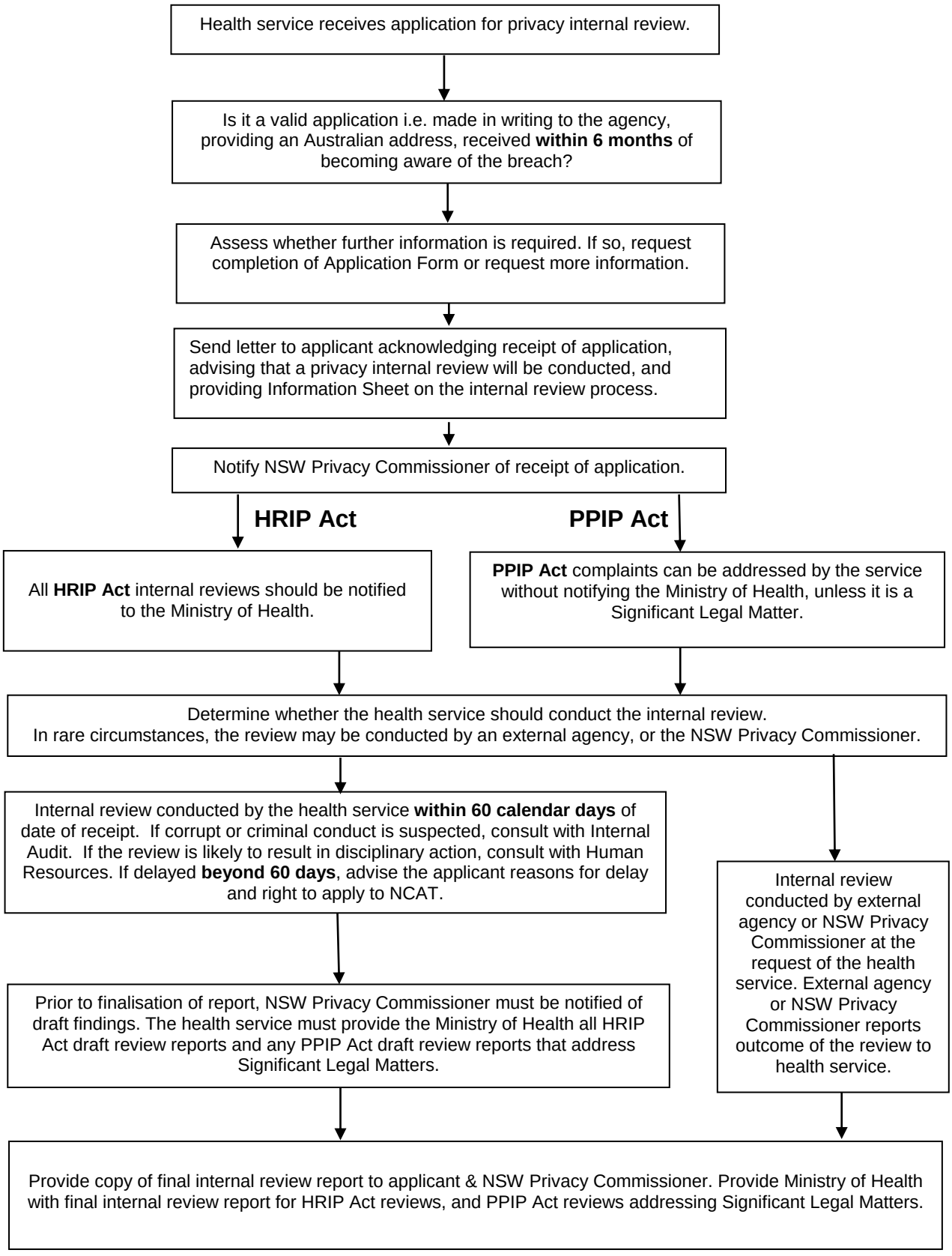
Appendix 5 Letters to the applicant

Appendix 6 Letter to NSW Privacy Commissioner notifying receipt of application

Appendix 7 Letter to NSW Privacy Commissioner providing draft report

Appendix 8 Template for privacy Internal Review Report

Appendix 1: Flow chart of the internal review process



Appendix 2: Checklist for privacy internal review

This form should be completed by the staff member overseeing the internal review

Reviewing Officer _____ Contact number _____

Role _____ Reference number _____

1. Is the complaint a matter which involves a possible breach of the *Privacy and Personal Information Protection Act 1998 (NSW), the Health Records and Information Privacy Act 2002 (NSW),* or a Code made under these Acts? If *yes*, proceed If *no,* address via normal complaints handling process.	YES / NO
2. Section 53 of the *Privacy and Personal Information Protection Act 1998* requires the application to be in writing, addressed to the health service concerned, specify an address in Australia and be lodged with the health service within 6 months (or such later date as the health service may allow) from the time the applicant became aware of the conduct. Has the applicant provided all information required? If *yes,* the date the applicant **became aware** of the conduct was:	YES / NO ___ / ___ / ___
3. Date of receipt of application for internal review	___ / ___ / ___
4. Date when the 60-calendar-day period for completion of the review will lapse	___ / ___ / ___
5. Identify the relevant Health Privacy Principle, Information Protection Principle, or other section of either Act or a Code of Practice:	HPPs: IPPs: Other:
6. Date when the letter of acknowledgement and a copy of Privacy Information Sheet was sent to the applicant	___ / ___ / ___
7. Date when the Privacy Commissioner was notified of the application and invited to make submissions, including a copy of the letter of acknowledgment to the applicant	___ / ___ / ___

8. Date draft review report sent to the Privacy Commissioner	___/___/___
9. 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 by NCAT within 28 calendar days of the review being completed	___/___/___
10. Possible criminal offences? (see below) If you have any concerns that the application may be about conduct that is criminal in nature, discuss the matter with Internal Audit. If a criminal offence may have been committed, the applicant should be advised to seek independent legal advice about reporting the conduct to the NSW Police Force.	YES / NO

Criminal offence time limits

The time limit for commencement of summary proceedings in a prosecution for corrupt disclosure or use of information under the HRIP Act or PPIP Act is **not later than 6 months** from when the offence was alleged to have been committed.

There are criminal offences relating to electronic data in the *Crimes Act 1900*. Section 308H of the *Crimes Act 1900* provides for a summary offence for unauthorised access to or modification of restricted data held in a computer. Proceedings under section 308H must be commenced **not later than 12 months** from when the offence was alleged to have been committed.

Appendix 3: Information sheet for privacy internal review

Privacy Internal Review

Privacy internal review is a process whereby this health service handles complaints about how it has dealt with personal information under the NSW *Privacy and Personal Information Protection (PPIP) Act 1998* and personal health information under the NSW *Health Records and Information Privacy (HRIP) Act 2002*.

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

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

The request for internal review should be lodged using an application form available from the health service, NSW Health or the NSW Information and Privacy Commission. This application should be sent directly to the health service within six months from the time the applicant first became aware of the conduct sought to be reviewed. If an application for internal review is received more than six months from the time the applicant became aware of the conduct, the health service will refuse to accept the application unless special circumstances apply.

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

A Review Officer will be appointed to conduct the internal review, which should be completed within 60 calendar days from the day on which the application is received by the health service. If the review is not completed within 60 calendar days, the health service will contact the applicant to explain the circumstances for the delay. If this occurs, the applicant is entitled to make an application to the NSW Civil and Administrative Tribunal to review the privacy complaint.

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 Ministry of Health. All information held by the health service in connection with the complaint will otherwise be kept secure and confidential.

The internal review must recommend that the health service 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 internal 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 health service including the reasons for taking that action, and
- the right of the applicant to have the findings of the review and proposed action of the health service reviewed by the NSW Civil and Administrative Tribunal (NCAT).

If an applicant is not satisfied with the findings of the internal review, or the action taken by the health service in relation to the application, the applicant may apply to NCAT for a review of the conduct that was the subject of the application. The application to NCAT must be made within 28 calendar days from being notified of the findings of the internal review.

[*Name and contact details of Privacy Contact Officer for relevant health service*]

Appendix 4: Privacy internal review application form

This is an application for review of conduct under:

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

Please choose one. If you seek to apply under both Acts, it is recommended that you submit two applications. See www.ipc.nsw.gov.au for further information on the two Acts.

1.	Name of the health service you are complaining about:
2.	Your full name:
3.	Your Australian postal address:
4.	Your phone number: Your email address: I agree to receive correspondence at the above email address.
5.	If you are complaining on behalf of someone else, please provide the following information about this person: Name: Postal address: Daytime telephone: Email: Describe your relationship to this other person e.g. parent, adult child, carer: Is the other person capable of making the complaint him or herself? ***Yes*** ***No*** ***I'm not sure*** Please provide proof that you have the legal authority to deal with the matter (guardianship order, power of attorney, their signed consent &/or proof of your relationship to the person).
6.	What is the specific conduct you are complaining about? Conduct may include an action or decision that has breached your privacy, or a failure to protect privacy. Your application should describe: • How your personal/health information was inappropriately collected; • How your personal/health information was inappropriately used or disclosed; • How your personal/health information is inaccurate; • How you were refused access to your personal/health information; • How the security of your personal/health information was compromised.

	Details of conduct complained about:
7.	When did the conduct occur? *(Please be as specific as you can)*
8.	When did you first become aware of this conduct? Please provide the date: ___/ ___ /_____ How did you become aware of the conduct?
9.	You need to lodge this application within 6 months of the date you have written at Q.8. *If more than 6 months has passed since you became aware of the conduct, you need to ask the health service 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:*
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 achieve from this review? Are you seeking a particular outcome (e.g. an apology, review of hospital policies)? This will be discussed with you as part of the internal review process.
13.	I understand that this form will be used by the health service to process my request for an internal review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with: • section 54 (1) of the *Privacy and Personal Information Protection Act 1998*, or • section 21 of the *Health Records and Information Privacy Act 2002* and that the Privacy Commissioner will be kept advised of the progress of the review. I would prefer the Privacy Commissioner to have: • a copy of this application form, or • just the information provided at Questions 6–12 (all identifying information be withheld from the Privacy Commissioner). If the review is not completed within 60 days from the day on which the application was received, you are entitled to a review by the NSW Civil and Administrative Tribunal. The health service will contact you about any delay, if necessary.
14.	**YOUR SIGNATURE:** **DATE :**
	SEND THIS FORM TO THE HEALTH SERVICE YOU NAMED AT QUESTION 1 **Keep a copy for your own records** This application form has been adopted with permission from Information and Privacy Commission NSW. This form is designed for your convenience. It is not a legal requirement that you complete this form.

Appendix 5: Letters to the applicant

Letters to the applicant may vary depending on the information provided in the initial application and other factors. The following templates may be adapted for use:

Appendix 5.1 Acknowledgement of receipt of application

Appendix 5.2 Letter to the applicant advising the application is out of time

Appendix 5.3 Letter to the applicant requesting an extension of time to complete the review

Once the Internal Review Report has been finalised and any submissions made by the NSW Privacy Commissioner have been considered, the health service should send a copy of the Internal Review Report to the applicant under the cover of the following letter:

Appendix 5.4 Letter to the applicant – Completed Internal Review Report

Appendix 5.1: Acknowledgement of receipt of application

APPLICANT'S NAME
APPLICANT'S ADDRESS Our ref:

Dear APPLICANT'S NAME

RE: Application for privacy internal review

I wish to acknowledge receipt of your application for privacy internal review by [*health service name*] on the [*date*].

In my role as Privacy Contact Officer and being independent of the circumstances surrounding your complaint, I will conduct this internal review for the [*health service name*].

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*].

[Optional, if the applicant has not completed a privacy internal review application form: Please find enclosed the NSW Health privacy internal review application form. While it is not obligatory, we would appreciate it if you could complete and return this form as soon as possible. It will assist us in better understanding your complaint.]

Under the law, [*health service name*] is allowed 60 calendar days to conduct the internal review from the day on which the application was received. As we received your application on [*date*], we will complete your internal review by [*date*].

We will contact you if for any reason the internal review has not been finalised by this date and explain the circumstances for the delay. Alternatively, if the internal review is not completed within 60 days, you may apply directly to the NCAT for an administrative review.

The law requires that the NSW Privacy Commissioner be notified of this application and be advised of the progress of the review. A copy of your application has been forwarded to the Office of the Privacy Commissioner. [*Delete this sentence if the applicant indicates they want to be anonymous. In such cases, a de-identified copy of the application should be provided to the NSW Privacy Commissioner with the applicant's consent*]

I enclose the Information Sheet for Privacy Internal Review and Privacy Leaflet for Patients [*or Privacy Leaflet for Staff, if relevant*].

If you have any questions relating to this matter, please do not hesitate to contact me on [*telephone number and email details*].

Yours sincerely

Name of Privacy Contact Officer/ Review Officer

Enclosures:
- Information Sheet for Privacy Internal Review
- Privacy Leaflet for Patients

[*Date*]

Appendix 5.2: Letter to the applicant advising the application is out of time

APPLICANT'S NAME
APPLICANT'S ADDRESS Our ref:

Dear APPLICANT'S NAME

RE: Your application for privacy internal review

In reference to your letter and application for privacy internal review dated [*date*], it is noted that you became aware of the alleged conduct which is the subject of the complaint on [*date*].

Section 53 of the *Privacy and Personal Information Protection Act 1998* states an application for a review of conduct must 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 which is the subject of the application.

It is noted that your complaint is outside of the six-month time limit, being approximately X months/years since the date you became aware of the alleged conduct.

[*Optional, if the application appears to have substance and the applicant has not completed an NSW IPC or NSW Health standard privacy internal review application form*:] In order for us to consider whether to accept your application outside of the six-month period, please provide us with your reasons for the delay in submitting the application (e.g. ill health, family trauma or other reasons). Your reasons should be provided to me by email or letter within 7 days.

[*If the applicant completed a standard internal review application form but failed to provide sufficient reasons for delay beyond 6 months*]:

As your application has not provided sufficient reasons to justify an extension of this time period, [*health service name*] is declining to accept your application for internal review and will not conduct an internal review pursuant to NSW privacy laws.

However, [*health service name*] will consider the issues raised by your complaint as part of our normal administrative processes.

I appreciate that this decision may cause you some concern and you are welcome to contact me if you have any questions relating to this decision please contact me on [*telephone number and email details*].

Yours sincerely

Privacy Contact Officer / Review Officer
[*Date*]

Appendix 5.3: Letter requesting an extension of time to complete the review

APPLICANT'S NAME
APPLICANT'S ADDRESS Our ref:

Dear APPLICANT'S NAME

RE: Extension of time to complete privacy internal review

I refer to your application for a privacy internal review by [*health service name*] received on [*date*]. As you are aware, the *Privacy and Personal Information Protection Act 1998* allows a health service 60 days to conduct the internal review from the day on which the application was received. This review was due to be completed on or before the [*date*].

It is regrettable that due to [*describe the circumstances*], I have not been able to complete your internal review and sincerely apologise for the delay. However, as discussed in our telephone conversation [*or via email*], I would like to request that an extension be granted so that the review can be completed to reflect a diligent process. I anticipate that the review will be completed by [*date*]. If there is to be any further delay, I will contact you prior to this revised completion date.

Given that the internal review was not completed within 60 days and you will not be provided with the outcome of review on time, you are entitled to make an application under section 55 of the *Privacy and Personal Information Protection Act 1998* to the NSW Civil and Administrative Tribunal for an administrative review of the conduct concerned. The contact details for the Tribunal are:

NSW Civil & Administrative Tribunal
Registry Administrative & Equal Opportunity Division
Level 10
John Maddison Tower
86-90 Goulburn Street
Sydney NSW 2000

Telephone: **1300 006 228** and select **Option 3**
Online at: www.ncat.nsw.gov.au

If you await the completion of the internal review, you are still entitled to seek a review of the conduct in the NSW Civil and Administrative Tribunal and you will be further advised of this when the internal review is completed.

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

Yours sincerely

Privacy Contact Officer / Review Officer
cc NSW IPC
[Date]

Appendix 5.4: Letter to the applicant – Completed Internal Review Report

APPLICANT'S NAME
APPLICANT'S ADDRESS Our ref:

Dear [NAME OF APPLICANT],

RE: Outcome of your application for privacy internal review

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*]. In summary, your complaint concerned [*briefly summarise 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. In summary, it is found that a breach of privacy principles in relation to your health / OR personal/ information has/ OR has not occurred. [*List the specific issues and summary of findings*]

If you are dissatisfied with the outcome of this review, the Act provides you with a right to lodge an appeal to the NSW Civil and Administrative Tribunal within 28 calendar days from receipt of this correspondence (+ 5 calendar days for postage). The Tribunal's contact details are:

NSW Civil and Administrative Tribunal
Registry Administrative & Equal Opportunity Division
Level 10
John Maddison Tower
86-90 Goulburn Street
Sydney NSW 2000

Telephone: **1300 006 228** and select **Option 3**
Online at: www.ncat.nsw.gov.au

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*], Privacy Contact Officer, [*health service name*] on [*telephone number and email details*].

Yours sincerely

Privacy Contact Officer / Review Officer
cc. NSW IPC
cc. Privacy Contact Officer, Legal and Regulatory Services Branch, NSW Ministry of Health (HRIP matters only)

Enclosed

- Copy of letter of notification to NSW Privacy Commissioner
- Privacy Internal Review Report

[*Date*]

Appendix 6: Letter to NSW Privacy Commissioner notifying receipt of application

[*Name of Privacy Commissioner*]
Privacy Commissioner
GPO Box 7011
Sydney NSW 2001 Our ref:

Via email: ipcinfo@ipc.nsw.gov.au

Dear [*Name of Privacy Commissioner*]

RE: Application for Internal Review by [*Name of applicant***]**

This is to advise that an application for an internal review was received by [*health service name*] 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 a health service 60 calendar days to conduct the internal review from the day on which the application was received, the [*health service name*] must complete the review by [*date*].

A copy of the application is attached for your reference. [*Note*: ensure the application is de-identified if requested by the applicant].

When the review is completed, I will provide you with a copy of the draft Internal Review Report for your consideration.

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 and email details*].

Yours sincerely

Privacy Contact Officer / Review Officer
cc. Privacy Contact Officer, Legal and Regulatory Services Branch, NSW Ministry of Health

[Date]

Appendix 7: Letter to NSW Privacy Commissioner providing draft report

[*Name of Privacy Commissioner*]
NSW Privacy Commissioner
GPO Box 7011
Sydney NSW 2001

Via email: ipcinfo@ipc.nsw.gov.au

Dear [*Name of Privacy Commissioner*]

RE: Draft Internal Review Report for [*Name of applicant***]**

Please find attached the draft Internal Review Report 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 1998*, the review must be completed by the [*health service name*] 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.

I am happy to discuss any aspects of this matter and can be contacted on [*provide telephone and email details*].

Yours sincerely

Privacy Contact Officer / Review Officer
cc. Privacy Contact Officer, Legal and Regulatory Services Branch, NSW Ministry of Health

[Date]

Appendix 8: Template for privacy internal review report

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 [*name of applicant*], ("the applicant").
Once you have written the applicant's name here once, the applicant should be referred to as "the applicant" for the rest of the document. This helps to distinguish the applicant from any witnesses and makes the Internal Review Report easier to read. It also makes it easier to de-identify the report should this be required.

The application relates to events that took place at [*describe location*] on [*describe time frame*].

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. Be mindful not to repeat details provided in Section 2. 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

Summarise:
- *when application was received*
- *when letter of receipt was sent to the applicant*
- *when Privacy Commissioner was advised*
- *when internal review was commenced*
- *chronology of relevant events.*

3. INTERNAL REVIEW

(Standard Text)
Two pieces of privacy legislation operate in NSW. *The Health Records and Information Privacy Act 2002* (HRIP Act) regulates "health information" through 15 Health Privacy Principles (or HPPs). The *Privacy and Personal Information Protection Act 1998* (PPIP Act) regulates general personal information (other than health information) through 12 Information Protection Principles and regulates the review of conduct by public sector agencies for both Acts.

Section 21 of the HRIP Act and 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*"*

Determine whether the application relates to "personal information" and indicate 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.

Determine whether the application relates to "personal health information" and indicate briefly why. State your conclusion:
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 Local Health District / Network the appropriate agency to deal with the complaint?

Ensure you have identified that your Local Health District / Network 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 "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. It may be helpful to quote relevant sections of the complaint.

4. ALLEGED BREACHES OF THE PPIP ACT 1998/ HRIP ACT 2002 [*delete as appropriate*]

List and summarise each of the Information Protection Principles / or Health Privacy Principles identified as relevant, and again quote sections of the complaint relevant to each principle. Then under 'Assessment of conduct' identify whether the health service's conduct has breached each Principle. For example:

4.1 Terms of Information Protection Principle or Health Privacy Principle

Insert actual wording of Privacy Principle (or refer to wording in an Attachment).

4.2 Assessment of conduct

Summarise outcome of review, refer to policies, patient leaflets and other relevant documents considered and identify whether the conduct in question has/has not breached the relevant privacy principle.

Set out information about the review process and analysis of the information and evidence that has been collected, addressing the following:

1. *Did the conduct occur and what is the evidence showing this?*
2. *If it is found that the conduct did occur, describe how the conduct amounts to a breach of an IPP/HPP.*
3. *Where no breach is found, describe how the conduct demonstrates compliance with privacy principles. Refer to relevant NSW Health privacy policies, local protocols, etc.*
4. *What is the extent of the breach? Consider the seriousness.*
5. *What is an appropriate response in light of a breach?*

This assessment should provide relevant information such as dates, information obtained during the course of the review such as audit reports, records of interview that includes factual accounts from individuals, any other supporting documents and records such as privacy undertakings. It is important to note that supporting documents should also include any information that demonstrates that a breach did not occur.

If the evidence of the breach is ambiguous, an assessment can be made as to whether on the balance of probabilities the facts have been established. A fact is proved on the balance of probabilities if its existence is more probable than not. For example, the report might state:

On the balance of probability, it has been determined that details of the applicant's health information were / were not disclosed by X to Y without the applicant's consent.

Conclude with the finding:
It is found that this Information Protection Principle / 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 Protection 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).

The report should clearly demonstrate to the applicant and the Privacy Commissioner how the reviewer has come to make the findings. This requires reference to information gathered in the internal review and how it establishes compliance or non-compliance with the IPPs/HPPs.

6. RECOMMENDATIONS

(Standard Text)
Section 53(7) of the *Privacy and Personal Information Protection Act 1998* sets out the list of possible recommendations that may be provided at the end of the internal review. These are to:

- take no further action on the matter
- make a formal apology to the applicant
- provide undertakings that the conduct will not occur again
- implement administrative measures to ensure that the conduct will not occur again (for example, revision of relevant policies and guidelines, and privacy training for relevant staff).
- take such remedial action as it thinks appropriate.

In this case, the applicant has sought:

Identify what the applicant has asked to occur, irrespective of whether it falls within the above categories.

Set out the recommendations arising out of the review. In doing so, have regard to what the applicant has asked for and the list of possible recommendations listed in the PPIP Act. If the review does not propose to act on the applicant's request(s), explain why in a neutral manner.

Where the applicant requests monetary compensation
In circumstances where an applicant requests money (for example, as compensation for a breach or for reimbursement of costs incurred as a result of a breach), the following approach is suggested:

If a breach has not occurred, then your recommendations would not include any offer of compensation, damages or reimbursement of costs.

If a breach of privacy has occurred, invite the applicant to provide evidence to substantiate a claim. The following statement could then be made in the internal review:

The applicant's request for compensation is noted. In view of the fact that the internal review has identified that there has been a privacy breach, the applicant may be eligible for compensation.

Compensation can only be provided in limited circumstances, for example, if the applicant has suffered loss or damage (financial, psychological or physical) as a direct result of the breach of privacy.

The applicant may write to the health service directly outlining the compensation sought. The applicant should attach receipts of expenses incurred to justify the claim. The health service will then contact its insurer and seek an early evaluation of the claim.

As outlined in the covering letter, if the applicant is dissatisfied with the health service's response, the Act provides a right to lodge an appeal to the NSW Civil and Administrative Tribunal within 28 calendar days from receipt of this correspondence (+ 5 calendar days for postage).

There are maximum financial limits for compensation claims. For more information, please refer to the website of the NSW Information and Privacy Commission: www.ipc.nsw.gov.au/privacy/privacy-resources-citizens/privacy-reviews