14 Complaints handling and responding to breaches

This chapter summarises considerations when handling privacy complaints and data breaches affecting health information. Breaches may be identified as a result of a consumer's privacy complaint or may also be identified by the health service before consumers are aware that their health information has been affected by a breach. This chapter summarises how to respond to consumer complaints and to breaches that are identified by the health service.

All privacy complaints, reports of privacy or data breaches, and requests for privacy internal review should be treated as serious matters and must be referred to the Privacy Contact Officer.

14.1 General complaint handling principles

People who have a privacy complaint against a health service should be informed of their right to make a formal application for a privacy internal review. Complainants should also be given the option to have the complaint addressed quickly and informally as an alternative to privacy internal review.

A formal complaint would generally include:

- a complaint submitted on an internal review application form, and/or
- correspondence which refers to the privacy internal review process, and/or
- correspondence which indicates that the applicant is aggrieved or dissatisfied with the treatment of their health information (and/or personal information) and the health service is unable to arrive at resolution through informal processes.

The *Health Records and Information Privacy Act 2002* requires health services to use the internal review process set out in Part 5 of the *Privacy and Personal Information Protection Act 1998*. Guidelines for management of complaints using these processes are set out in *NSW Health Privacy Internal Review Guidelines (GL2019_015)*. If health services receive a complaint under privacy legislation, this Guideline must be referred to and the local privacy contact officer notified of the complaint.

Staff must also notify complaints in the NSW Health incident management system and follow the procedures outlined in the *Incident Management Policy Directive (PD2020_047)*.

In circumstances where the HCCC has requested that a health service respond to a complaint which involves both clinical and privacy issues, the health service should address the privacy issues as comprehensively as possible in response to the HCCC complaint. In addition, the health service should advise the HCCC that the aggrieved person is also entitled to seek a privacy internal review from the relevant health service regarding the privacy aspects of the complaint. The privacy internal review application form and the privacy internal review information sheet should be enclosed with the response to the HCCC, together with the appropriate contact details for the health service.

14.2 Privacy internal reviews

Individuals can make a complaint about a health service's management of health information on the grounds that the health service has contravened a Health Privacy Principle or a Health Privacy Code of Practice. Such complaints should be referred immediately to the agency's Privacy Contact Officer (see Section 6.2).

The focus of an internal review is the conduct of the agency concerned:

> *A person (**the applicant**) who is aggrieved by the conduct of **a public sector agency** is entitled to a review of that conduct.*

On receipt of a Privacy Internal Review application, guidance can be sought from the Ministry of Health privacy team and the *NSW Health Privacy Internal Review Guidelines (GL2019_015)*

Any privacy complaint must be in writing, addressed to the health service concerned and made within six months of the individual becoming aware of the alleged contravention (unless the health service agrees to a longer timeframe). See Section 4.4 of the *NSW Health Privacy Internal Review Guidelines (GL2019_015)* for further guidance.

A person is not required to identify the particular HPP which is the subject of the complaint. Health services are obliged to review any such complaint received and to identify the specific HPPs which may have been breached. The internal review provisions allow individuals to seek a review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the privacy laws.

Where a person raises general concerns as to how health information is being handled and does not indicate that they are personally aggrieved by the conduct, agencies should seek to address the person's concerns by reference to the agency's existing information management policies and guidelines for complaints handling. For example, a patient may express concern about the number of staff accessing patient health records. The patient may be seeking an explanation and reassurance regarding staff duties of confidentiality, rather than a privacy internal review of this practice.

Where the person's concerns cannot be resolved through referring to existing policies and guidelines, an agency must provide the person with information relating to their rights to an internal review under privacy law, and the requirements for lodging a valid application.

In some cases, the privacy complaint may relate to, or be linked with other complaints lodged with the health service. When this occurs, the privacy officer should alert the decision maker and vice versa, so that the two investigation processes can be managed concurrently.

An individual may also complain on behalf of someone else if they are authorised to act on their behalf (for example, with the applicant's consent or if they are a parent or guardian), or an individual may complain if they are aggrieved by the handling of someone else's personal or health information and such a complaint may also require a privacy internal review.

Further guidance:

- *NSW Health Privacy Internal Review Guidelines (GL2019_015)*, see Section 4
- *IPC Fact Sheet – making a complaint about a NSW public sector agency*

14.3 NSW Civil and Administrative Tribunal (NCAT)

If the complainant is not satisfied with the outcome of the internal review, the complainant may appeal to the NSW Civil and Administrative Tribunal (NCAT).

Where a complainant lodges an application to NCAT, the health service should notify:

- the NSW Ministry of Health Legal Unit at: moh-significantlegalmatters@health.nsw.gov.au
- Privacy Contact Officer, Ministry of Health, at: moh-privacy@health.nsw.gov.au
- the Treasury Managed Fund (TMF).

If the Tribunal finds the complaint against the health service proven, it may order the health service:

- to pay damages of up to $40,000 to the applicant by way of compensation for any loss or damage suffered because of the conduct
- to refrain from any conduct or action in contravention of an HPP
- to comply with an HPP
- to correct information which has been disclosed, and/or
- to take specified steps to remedy any loss or damage suffered by the applicant.

Further guidance:

- *NSW Health Privacy Internal Review Guidelines (GL2019_015)*

14.4 Responding to data breaches

A data breach involving personal health information occurs when there is an unauthorised access, disclosure or loss of that information. A data breach does not need to be caused by a deliberate or willful act. When a data breach occurs, the organisation no longer controls the personal health information for which it is responsible.

NSW Health organisations must implement the minimum standards outlined in the *Data Breaches involving Personal or Health Information (PD2023_040)* when responding to data breaches affecting personal health information or personal information.

The NSW Mandatory Notification of Data Breach (MNDB) scheme applies to data breaches affecting personal health information or personal information which involve a risk of serious harm. The scheme mandates notification of eligible data breaches to the NSW Privacy Commissioner and affected individuals.

Further guidance:

- *Data Breaches involving Personal or Health Information (PD2023_040)*

14.5 Breach of privacy by an employee

Where it is found, or suspected, that a staff member has breached one or more of the Health Privacy Principles (HPPs), the health service should investigate the allegations in accordance with the requirements for privacy internal review in order to determine:

- Whether a breach has occurred
- The nature and extent of the breach
- Whether the breach occurred inadvertently or deliberately
- What course of action to take with regards to the staff member
- Whether to notify the affected individuals (if they were not the complainant).

An internal review will determine whether such a privacy breach was attributable to the operation of the health service. Privacy breaches caused by employees when they are acting in their personal capacity rather than in their work or professional role may not be attributable to the health service if it has exercised all reasonable care to prevent breaches through measures such as privacy training, education and appropriate information security safeguards. However, the matter may warrant a misconduct investigation into the employee's conduct.

Referral of staff to Workforce must be considered in any incident of unauthorised staff access to health information. Where it is found, or suspected, that a staff member has used or disclosed health information without authorisation the health service should investigate the allegations in accordance with the NSW Health Policy directive, *Managing Misconduct (PD2018_031).*

When a breach of privacy by an employee is confirmed, action taken by the health service should be commensurate with the nature, scale and seriousness of the breach. Action can range from counselling or training to formal disciplinary action (warning, termination). Any actions must comply with relevant NSW Health policies.

Further guidance:

- *Managing Misconduct (PD2018_031)*
- *Managing Complaints or Concerns about Clinicians (PD2018_032)*
- *Public Interest Disclosures (PD2023_026)*
- *NSW Health Privacy Internal Review Guidelines (GL2019_015)*