14 Complaints handling

Health services should always try to resolve information privacy complaints quickly and informally, using formal processes as a last resort. However, privacy law provides patients with a right to make a formal complaint.

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 (and/or personal) information and the health service is unable to arrive at resolution through informal processes.

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 patient 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 information sheet should be enclosed with the response to the HCCC together with the appropriate contact details for the health service.

The *Health Records and Information Privacy Act 2002* requires health services to use the complaints 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 Internal Review Guidelines. If you receive a complaint under privacy legislation, you should refer to this document.

14.1 General principles

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

All privacy complaints, enquiries about privacy, and requests for internal review, should be treated as serious matters. A 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).

A person is not required to identify the particular HPP that he or she considers has been breached. Health services are obliged to review any such complaint received and to identify the specific HPPs which arise.

Privacy law provides first for a health service to conduct an internal review of a complaint. The internal review provisions allow individuals to seek a review of certain conduct of an agency, in circumstances where the individual believes that the agency has breached the terms of the privacy laws. Internal reviews are to be undertaken in accordance with the NSW Health Internal Review Guidelines which reflect the provisions of the *PPIP Act* and are based on guidelines issued by Privacy Commission NSW.

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

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

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.

14.1.1 NSW Civil & Administrative Tribunal (NCAT)

If the complainant is not satisfied with the outcome of the application, the complainant may then appeal the issue to the NSW Civil & Administrative Tribunal (NCAT).

Where a person lodges an action before the NCAT, the health service should notify the NSW Ministry of Health Legal and Regulatory Services Branch of the application, and a notification should also be made to the Treasury Managed Fund (TMF).

Further guidance

- GL2006_007: NSW Health Internal Review Guidelines

14.2 Sanctions

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 a HPP
- to comply with a HPP
- to correct information which has been disclosed and/ or
- to take specified steps to remedy any loss or damage suffered by the applicant.

There are also criminal offences relating to **public sector officials** found guilty of intentionally disclosing or using personal health information. Penalties include:

- the individual to pay a fine of up to $11,000 or to be imprisoned for up to 2 years, or both
- to confiscate any money or other benefit alleged to have been obtained by the individual in connection with the offence.

14.3 Notifying individuals of a breach of their privacy

From time to time, a health service may become aware that an individual's privacy has been breached. This may have occurred deliberately, for example, by a staff member inappropriately accessing health records, or inadvertently, for example, when the wrong 'Mrs Jones' is contacted by a health service, personal information is uploaded to the internet in error, or clinical hand-over notes are found in a public place.

There is no obligation within the *Health Records and Information Privacy Act 2002* or any law, to notify the individual when their privacy has been breached. However, as a matter of good practice, consideration should be given as to whether the affected individual(s) should be notified.

When notifying individuals of a breach of their privacy, the health service should provide them with the opportunity to apply for privacy internal review in accordance with the NSW Health Internal Review Guidelines.

In general, 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 privacy breach, the affected individuals should be notified. Risk of harm can include psychological, physical, financial or other. The health service should also notify the Ministry of Health which may notify the Information and Privacy Commission NSW.

Further guidance

- The Office of the Australian Information Commissioner has published the 'Data Breach Notification – A guide to handling personal information security breaches – April 2012', available at: www.oaic.gov.au/publications/

Whilst NSW Health is not obliged to comply with this document, it is a useful guide to assist health services in this area.

14.4 Breach of Health Privacy Principle(s) 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 individual(s) (if they were not the complainant), see Section 14.3.

When the finding constitutes a breach of privacy, action taken by the health service should be commensurate with the nature, scale and seriousness of the breach. Action can range from remedial (discussion, counselling, training) to disciplinary (warning, termination). However, any action should always comply with NSW Health policy and be managed in accordance with policy obligations.

Further guidance

- PD2005_225: Disciplinary Process in NSW Health – Framework for Managing the Disciplinary Process
- PD2006_007: Complaint or Concern about a Clinician
- GL2006_007: NSW Health Internal Review Guidelines