

Privacy Management Annual Report 2014-15

Western Sydney Local Health District (WSLHD) meets its privacy obligations through appropriate governance and the provision of privacy information, training and support to staff. Oversight for monitoring compliance with privacy legislation continues to be provided by the Privacy and Information Compliance Manager (Privacy Contact Officer).

WSLHD provides ongoing privacy information and support to its staff through:

- A privacy intranet website which provides all staff with access to:
 - NSW privacy legislation
 - NSW Health privacy policies (Health Information Privacy Manual and Internal Review Guidelines)
 - Privacy education and training
 - Links to external resources such as the Privacy and Information Commissioner
- Provision of privacy awareness at new staff orientation
- Provision of mandatory privacy training, available to staff as either on-line via HETI or face-to-face training programs
- Access to privacy information posters and patient information privacy leaflets, a copy of which is made available to all patients/clients attending a WSLHD facility.

The Privacy and Information Compliance Manager provides support and advice to WSLHD staff in relation to compliance with privacy legislation with particular reference to electronic health records (eMR) and access, use and disclosure of personal health information. There is a growing focus on education and training in relation to the use of social media by staff.

Privacy information is provided to consumers through

- an Information Privacy Internet site at <http://www.wslhd.health.nsw.gov.au/Quality---Patient-Safety/Right-to-Information/Information-Privacy/Information-Privacy>.
- The NSW Information Privacy Leaflet for Patients which is provided to all patients on entry to a health care facility
- The NSW Information Privacy Leaflet for Patients is available to patients/clients in patient care and public areas of the health care facilities.
- The NSW privacy poster is on display in patient care and public areas of the health care facilities.

The availability of privacy posters and leaflets to patients/clients is regularly audited. The last audit was performed in 2013 and a number of recommendations are currently being implemented. The next audit will be performed in 2015/16.

The Privacy and Information Compliance Manager has participated in the NSW Health Privacy Contact Officers Network Group meetings in 2014-15 where information privacy matters affecting business practice in NSW Health are discussed.

The *Privacy and Personal Information Protection Act 1998* and the *Health Records and Information Privacy Act 2002* provide the legislative framework and process for managing privacy complaints. The process is known as 'Internal Review'.

Actions which may be undertaken as a result of the Internal Review, include education and training; staff counselling; disciplinary procedures and revision of policy and procedure.

Privacy complaints where the complainant has not requested an Internal Review, or where the breach has been internally identified, are investigated using a modified approach of the internal review system. Thorough investigation is undertaken in all cases and any recommendations are implemented.

Privacy Internal Review

During 2014-15, WSLHD received two new applications for Internal Review:

1. Application for Internal Review received October 2014. Staff member alleging multiple breaches of privacy by her manager. Breach of *IPP10 Limits on use of personal information* was proven. Staff were counselled. Matter was referred to NCAT in combination with second privacy matter for this complainant (2).
2. Application for Internal Review received in December 2014 from staff member (same staff member in 1). Staff member alleged her privacy had been breached in corporate record keeping system (TRIM). Breaches of *IPP 10 Limits on use of personal information* and *IPP 5 Retention and security of personal information* were proven. Changes to corporate records management and use of security were implemented in the business unit. Matter was referred to NCAT in combination with first privacy matter for this complainant (1). Both matters were settled for \$8,000.
3. Application for Internal Review received in December 2014 from five members of the same family alleging a breach of privacy by a staff member who was an ex-family member. Internal review found breach of *HPP 5 Retention and security*. Matter was referred to NCAT where no breach of *HPP 5 Retention and security* was found. Further no breach of *HPP 10 Limits on use of personal health information* or *HPP 11 Limits on disclosure of personal health information* was found. Matter was settled for \$5,000 for the five applicants.
4. Application for Internal Review received in July 2015 from patient alleging a breach of privacy by a staff member who was her former partner. Internal Review found breach of *HPP 10 Limits on use of health information*. Staff member was terminated.

Privacy Breaches

During 2014-15, WSLHD received one complaint in relation to a breach of privacy, not requesting Internal Review, and one alleged breach of privacy was identified via internal systems. The nature of these matters and outcomes are as follows:

1. Carried over from May 2014. Internally identified breach of privacy. Staff member inappropriately accessing Cerner health care records. Breach of *HPP 10(1) Limits on use of health information* was proven. Staff member recommended for termination however decision makers recommended first warning and counselling.
2. July 2014 – Internally identified breach of privacy. Staff member alleged to have disclosed details related to confidential investigation. Breaches unable to be substantiated. No further action. File closed.
3. August 2014 - complaint received from former patient alleging breach of privacy by staff member. Staff member and complainant are known to each other socially. Breach of *HPP 10 Limits on use of personal health information* was proven. Staff member recommended for termination but resigned before termination could be effected. Staff member placed on Service Check Register.
4. October 2014 - staff member had copy of patient notes in bag that was stolen and not found. Notification was made to patient, in writing with formal complaint form attached. No complaint received. Staff member counselled in relation to taking patient notes off site. File closed.
5. November 2014 – internally identified breach of privacy. Staff member inappropriately accessing Cerner health care records. Breach of *HPP 10(1) Limits on use of health information* was proven. Staff member was terminated and placed on Service Check Register.